

2

الهاكر الأخلاقي

عملية الاستطلاع (RECONNAISSANCE)

By

Dr.Mohammed Sobhy Teba
RECONNAISSANCE
https://www.facebook.com/tibea2004

CONTENTS

(مفهوم فوت برنت) FOOTPRINTING CONCEPTS 2.1

مقدمه

المصطلح **RECONNAISSANCE** بالتعريف يأتي من استراتيجية الحرب العسكرية لاستكشاف خارج المنطقة المحتلة من قبل القوات الصديقة للحصول على معلومات عن العدو للتحليل أو لهجوم مستقبلي. أما هنا في أنظمة الكمبيوتر فانه مشابه لذلك، وهذا يعني عادة أن مختبر الاختراق "**Penetration testing**" او الهاكر سوف يحاول معرفة أكبر قدر ممكن حول البيئة الهدف وصفات النظام قبل شن الهجوم. وتعرف أيضا هذه العملية باسم **Footprinting**. عملية الاستطلاع هو عادة في الحقيقة غير شرعي وفي كثير من الحالات (ومع ذلك، نحن لسنا محامين، ولا يمكن تقديم المشورة القانونية) لأنك تتعامل مع نظام غير مصرح لك به. أمثلة على عملية الاستطلاع تشمل أي شيء من البحث على مصادر عامة عن الهدف مثل جوجل، ورصد نشاط الموظفين لمعرفة أنماط التشغيل، ومسح/فحص الشبكات أو الأنظمة لجمع المعلومات، مثل نوع التصنيع، ونظام التشغيل، ومنافذ الاتصال المفتوحة. لمزيد من المعلومات التي يمكن جمعها حول هدف يجلب فرصة أفضل لتحديد أسهل وأسرع الطرق لتحقيق هدف الاختراق، فضلا عن أفضل طريقة لتجنب النظام الأمني القائم. أيضا، تنبيه الهدف من المرجح أن يسبب بعض السبل لغلق الهجوم كرد فعل على التحضير للهجوم. ومن الاقوال الشهير: "كلما كنت أكثر هدوء، كلما كنت قادرا على السمع "

ينبغي أن تسجل نتائج عمليات الاستطلاع في وثائق سريه، وذلك لأن البيانات الموجودة قد تكون ذات صلة في وقت لاحق في ممارسة الاختراق. أيضا سوف يحتاجها العملاء وذلك لأنهم يريدون أن يعرفوا كيف تم الحصول على مثل هذه البيانات، ويطلبون المراجع لهذا. ومن الأمثلة على ذلك الأدوات التي تستخدم للحصول على البيانات أو مورد ما، على سبيل المثال، استعلام بحث معين في محرك البحث **Google** الذي تم تقديمه للحصول على البيانات. إعلام العميل "بانك حصلت على المعلومات" ليست جيدة بما فيه الكفاية، لأن الغرض من اختبار الاختراق هو تحديد نقاط الضعف للإصلاحات في المستقبل.

(مصطلحات فوت برنتنج) FOOTPRINTING TERMINOLOGY

قبل الذهاب قدما إلى عمق هذا المفهوم وكيفية استخدامه، سوف نتعرف أولا على بعض المصطلحات الأساسية المستخدمة في **Footprinting**. هذه المصطلحات تساعدك على فهم مفهوم Footprinting وهيكلتها.

OPEN SOURCE OR PASSIVE INFORMATION GATHERING (OSINT)

هذه الطريقة تعتبر من الطرق السهلة في جمع المعلومات عن الهدف. وهي تشير إلى عملية جمع المعلومات من المصادر المفتوحة أي من المصادر العامة المتاحة وهذه المعلومات تكون متاحه للجميع. هذا النوع لا يدعم الاتصال المباشر بالهدف وقانونيي.

المصادر المفتوحة/المجانية للمعلومات تشمل الاتي: الجرائد والتلفزيون ومواقع التواصل الاجتماعي مثل فيسبوك و**blogs** والخرائط وجوجل وغيرها.

باستخدام هذا النوع يمكنك تجميع المعلومات مثل نطاق الشبكة (**network range**) وعناوين **IP** القابلة للوصول على الإنترنت ونظام التشغيل وتطبيقات خوادم الويب التي يتم استخدامها بواسطة الشبكة الهدف وبروتوكولات النقل سواء **UDP** أو **TCP** وأليات التحكم في الوصول وبنية النظام وأنظمة كشف التسلل وهكذا.

ACTIVE INFORMATION GATHERING

في هذا النوع من جمع المعلومات فإن المهاجمين يقومون بالتركيز أساسيا على موظفي المنظمة الهدف. بحيث يحاولون انتزاع بعض المعلومات من هؤلاء الموظفين عن طريق استخدام الهندسة الاجتماعية. هنا يتم التعامل مباشرة مع المنظمة الهدف.

ANONYMOUS FOOTPRINTING

هذا يشير إلى عملية جمع المعلومات من مصادر مجهولة.

PSEUDONYMOUS FOOTPRINTING

هذا يشير إلى عملية جمع المعلومات من مصادر تم نشرها على شبكة الإنترنت ولكن غير مرتبطة مباشرة باسم الكاتب. حيث يمكن نشر المعلومات تحت اسم مختلف أو الكاتب قد يكون له اسم مستعار مشهور أو قد يكون الكاتب مسئول في احدى الشركات أو الجهات الحكومية

ويحظر عليه النشر تحت اسمه الحقيقي أو الأصلي. ويسمى هذا النوع بغض النظر عن السبب في إخفاء الاسم الحقيقي وجمع المعلومات من هذه المصادر يسمى pseudonymous.

ORGANIZATIONAL OR PRIVATE FOOTPRINTING

هذا النوع يشمل جمع المعلومات من تقويم المنظمات على شبكة الإنترنت ومن خلال خدمات البريد الإلكتروني.

INTERNET FOOTPRINTING

هذا يشير إلى عملية جمع المعلومات من المنظمة الهدف من خلال اتصال هذه المنظمة بشبكة الإنترنت.

ما هو الفوت برنتنج (FOOTPRINTING)؟

F هو أول مرحله من مراحل القرصنة الأخلاقية. والتي تشير إلى عملية جمع المعلومات عن الشبكة الهدف والبيئة المحيطة بها. باستخدام **Footprinting** يمكنك إيجاد طرق عده للتطفل على الشبكة الهدف وهو يعتبر **methodological** أي له منهجيه في العمل وذلك بسبب أن سعته للمعلومات الهامة كان على أساس المنهجيات السابقة.

بمجرد أن تبدأ عملية **Footprinting** بطريقة منهجية، فإنك سوف تحصل على مخطط (**blueprint**)للأمن الشخصي للمنظمة المستهدفة. هنا يتم استخدام المصطلح '**blueprint**' لأن النتيجة التي سوف تحصل عليها في نهاية **Footprinting** يشير إلى وضع النظام الفريد للمنظمة الهدف.

ليس هناك منهجية واحدة لل **Footprinting** كما أنه يمكنك تتبع المعلومات بطرق عده. ومع ذلك، فإن هذا لا يقل أهمية عن احتياجاتك لجميع المعلومات الحاسمة التي يتعين جمعها قبل أن تبدأ عملية القرصنة. وبالتالي، يجب أن تنفذ **Footprinting**بدقة وبطريقة منظمة.

يمكنك جمع المعلومات عن المنظمة المستهدفة من خلال وسائل Footprinting في أربع خطوات:

1. جمع المعلومات الأساسية حول الهدف وشبكتها.
2. تحديد نظام التشغيل المستخدم، ومنصات التشغيل، وإصدارات خادم الويب، الخ.
3. يؤدي بعض التقنيات مثل **Whois**و**DNS** و **network and organizational queries**.
4. البحث عن الثغرات الأمنية واستخدامها في الهجوم.

علاوة على ذلك، سوف نناقش لاحقا كيفية جمع المعلومات الأساسية، وتحديد نظام التشغيل من الكمبيوتر الهدف، منصات التشغيل، وإصدارات خادم الويب، وأساليب مختلفة من**Footprinting** ، وكيفية إيجاد واستغلال نقاط الضعف بالتفاصيل.

لماذاFOOTPRINTING ؟

Footprinting يتم استخدمها من قبل المهاجمين لبناء استراتيجية القرصنة، والحاجة إلى جمع المعلومات عن شبكة المنظمة الهدف، حتى يتمكنوا من العثور على أسهل طريقة لاقتحام محيط أمن المنظمة. كما ذكر سابقا، **Footprinting**هو أسهل طريقة لجمع المعلومات عن المنظمة المستهدفة، وهذا يلعب دورا حيويا في عملية القرصنة. **Footprinting**يساعد على الاتي:

- **معرفة الوضع الأمني (know security posture)**

أداء***Footprinting*** على المنظمة الهدف بطريقة منتظمة ومنهجية يعطي صورة كاملة عن الوضع الأمني للمنظمة. بحيث يمكنك تحليل هذا التقرير لمعرفة الثغرات في الوضع الأمني للمنظمة التي تستهدفها وعلى ذلك يمكنك بناء خطة الهجوم.

- **الحد من منطقة الهجوم (Reduce Attack Area)**

باستخدام مجموعة من الأدوات والتقنيات، فان المهاجمين يمكنهم استهداف كيان غير معروف (على سبيل المثال منظمة**XYZ**) وتقليص هذا الكيان إلى مجموعة محددة من أسماء الدومين (**domain names**)، وكتل الشبكة، وعناوين **IP** الفردية للأنظمة المرتبطة مباشرة إلى شبكة الإنترنت، وكذلك العديد من التفاصيل الأخرى المتعلقة بالموقف الأمني .

- **بناء قاعدة معلومات (Build Information Database)**

يوفر ***Footprinting***أقصى قدر ممكن من المعلومات التفصيلية عن المنظمة المستهدفة . حيث يقوم المهاجمين ببناء قاعدة بيانات من المعلومات الخاصة بنقاط الضعف في نظام الأمن في المنظمة المستهدفة. ثم تحليل قاعدة البيانات هذه للعثور على أسهل طريقة لاقتحام نظام الأمن لهذه المنظمة.

- رسم خريطة للشبكة (Draw Network Map)

الجمع بين تقنيات ال *Footprinting* وبعض الأدوات مثل ترسرت (*Tracert*)يسمح للمهاجم إنشاء مخطط للشبكة مع وجود شبكة المنظمة الهدف. فان هذه الخريطة تمثل فهم لشبكة الإنترنت الخاصة بالهدف بواسطة **Footprint**. ويمكن لهذه الرسومات التخطيطية للشبكة توجيه الهجوم.

الهدف من عملية الاستطلاع (FOOTPRINTING)

الأهداف الرئيسية لل *Footprinting* تشمل الاتي جمع المعلومات عن الشبكة الهدف(**target's network information**) ، ومعلومات عن أنظمة التشغيل (**system information**)، ومعلومات عن المنظمة نفسها (**Organizational information**). من خلال تنفيذ *Footprinting* في مستويات الشبكة المختلفة، يمكنك الحصول على معلومات مثل: كتل الشبكة، خدمات الشبكة والتطبيقات، وبنية النظام، وأنظمة كشف التسلل، وعنوان **IP** المحدد، وآلية مراقبة الدخول. مع معلومات *Footprinting*، مثل أسماء الموظفين، وأرقام الهاتف وعناوين الاتصال، والخبرة في العمل، وهلم جرا من المعلومات التي يمكنك الحصول عليها.

- **جمع المعلومات عن الشبكة الهدف (target's network information):**

يمكن جمع المعلومات عن الشبكة الهدف عن طريق إجراء تحليل لقاعدة البيانات بواسطة **Whois**، و**trace routing**، الخ ويشمل الاتي: (اسم الدومين – اسم الدومين الداخلي – بلوكات الشبكة– عناوين IP للأنظمة التي يمكن الوصول إليها – **Rogue/private websites** – بروتوكولات النقل سواء **TCP** و**UDP** التي تعمل – ألية التحكم في الوصول (**Access control mechanisms**) و**ACLs** – بروتوكولات الشبكة – **VPN points** – جدار الحماية **IDSes** – أرقام التليفونات سواء **analog** أو **digital** – عمليات الولوج المشفرة (**authentication mechanism**) -نظام التعداد(**system enumeration**))

- **جمع معلومات عن أنظمة التشغيل (collect system information):**

أسماء المستخدمين والمجموعات التي ينتمون لها (**user** & **group name**) – جداول روتنج (**routing table**) – **SNMP** – هيكلة/نوع النظام – نوع remote system – اسم النظام – كلمات السر -system banner (نظام الإنذارات).

- **معلومات عن المنظمة نفسها (Organizational information):**

عناوين وأرقام التليفونات – تفاصيل عن الموظفين – مكان الشركة – دليل الشركة – خلفيه عن المنظمة – الأخبار الخاصة بالمنظمة – الموقع الرسمي للشركة – اتجاه الشركة – شهرة المنظمة – التعليقات الموجودة في الملفات المصدرية في **HTML**.

2.2 التهديدات الناتجة من عمليات الاستطلاع FOOTPRINTING THREATS

كما تم شرحه سابقا، فإن المهاجم يؤدى عملية الاستطلاع (**Footprinting**) كخطوه أولى في محاولة لاختراق المنظمة الهدف. في مرحلة عملية الاستطلاع (**Footprinting**)، فإن المهاجمون يحاولون جمع المعلومات القيمة على مستوى النظام مثل تفاصيل الحساب، ونظام التشغيل وإصدارات البرامج الأخرى وأسماء الخادم، وتفاصيل مخطط قاعدة البيانات التي من شأنها أن تكون مفيدة في مرحلة القرصنة.

فيما يلي مختلف التهديدات التي تكون بسبب عملية الاستطلاع (FOOTPRINTING).

1. **Social engineering الهندسة الاجتماعية**

بدون استخدام أية من أساليب التسلل، فإن المهاجمين يعملون على جمع المعلومات مباشرة وغير مباشرة من خلال الإقناع ومختلف الوسائل الأخرى. هنا، يتم جمع المعلومات الحاسمة من قبل المتسللين من خلال الموظفين دون تناسق بينهم.

2. **System and Network Attacks**

عملية الاستطلاع (**Footprinting**) يساعد المهاجم لتنفيذ هجمات النظام والشبكة. من خلال **Footprinting**، يمكن المهاجمين جمع معلومات ذات صلة بالمنظمة الهدف كملفات إعداد النظام، نظام التشغيل الحالي على الجهاز، وهلم جرا. باستخدام هذه المعلومات، يمكن عثور المهاجمين على نقاط الضعف الموجودة في النظام الهدف ومن ثم استغلال هذه الثغرات الأمنية. وبالتالي، يمكن المهاجمين من السيطرة على النظام الهدف. وبالمثل، يمكن للمهاجمين أيضا السيطرة على الشبكة بالكامل.

3. تسريب المعلومات Information leakage

تسريب المعلومات يمكن أن يشكل تهديدا كبيرا لأية منظمة وغالبا ما يتم تجاهله. بحيث إذا وقعت بعض من المعلومات الحساسة الخاصة بمنظمة ما في أيدي المهاجمين، ثم يقوموا ببناء خطة الهجوم على أساس هذه المعلومات، أو استخدامه للحصول على مبالغ نقدية.

4. فقدان الخصوصية Privacy Loss

مع مساعدة من عملية الاستطلاع **Footprinting**، فإن المهاجمين يمكنهم الوصول إلى الأنظمة والشبكات للشركة وحتى التصعيد من امتيازات تصل إلى مستويات الإدارة (**Admin privilege**). مهما كانت الخصوصية التي تحتفظ بها الشركة فإنها فقدت تماما.

5. تجسس الشركات corporate espionage

تجسس الشركات هي واحدة من التهديدات الرئيسية للشركات كمنافسين يمكنهم التجسس ومحاولة سرقة البيانات الحساسة من خلال **Footprinting**. بسبب هذا النوع من التجسس، فإن المنافسين قادرين على إطلاق منتجات مماثلة في السوق، مما يؤثر على الموقف السوقي للشركة.

6. الخسائر التجارية Business Loss

عملية الاستطلاع (**Footprinting**) له تأثير كبير على الشركات مثل شركات الإنترنت والمواقع الإلكترونية الأخرى، والأعمال المصرفية والشركات المالية ذات الصلة، وما إلى ذلك. المليارات من الدولارات يتم خسارتها كل عام بسبب الهجمات الضارة من قبل قراصنة.

2.3 منهجية/نظرية عمل عملية الاستطلاع FOOTPRINTING METHODOLOGY

منهجية الـ **Footprinting** هي وسيلة إجرائية لجمع المعلومات عن المنظمة الهدف من جميع المصادر المتاحة. إنها تتعامل مع جمع المعلومات عن المنظمة المستهدفة، وتحديد **URL** والموقع وتفاصيل إنشاء، وعدد الموظفين، ومجموعة محددة من أسماء الدومين، ومعلومات الاتصال. يمكن جمع هذه المعلومات من مصادر مختلفة مثل محركات البحث وقواعد البيانات **Whois**، الخ
محركات البحث (**search engines**) هي مصادر المعلومات الرئيسية حيث يمكنك العثور على معلومات قيمة عن المنظمة التي تستهدفها. لذا، أولا سوف نناقش **Footprinting** عن طريق محركات البحث. هنا نحن ذاهبون لمناقشة كيف وماذا يمكننا فعله من جمع المعلومات من خلال محركات البحث

فيما يلي العمليات التي يمكن القيام بها لجمع المعلومات والتي سوف نتحدث عنها في هذا الجزء.



FOOTPRINTING THROUGH SEARCH ENGINES-1 عملية الاستطلاع باستخدام محركات البحث

تم تصميم محركات البحث (**search engine**) على شبكة الإنترنت للبحث عن المعلومات على شبكة الويب العالمية. يتم عرض نتائج البحث بشكل عام في خط من النتائج ويشار إليها بصفحات نتائج محرك البحث(**Search Engine Result Pages SERPs**) . في العالم الحاضر، العديد من محركات البحث تسمح لك بانتزاع المعلومات عن المنظمة الهدف مثل منصات التكنولوجيا وتفاصيل الموظفين، صفحات تسجيل الدخول، و**internet gateway**، وهكذا. باستخدام هذه المعلومات، فان المهاجم يقوم ببناء استراتيجية القرصنة لاقتحام شبكة المنظمة المستهدفة ومن الممكن تنفيذ أنواع أخرى من هجمات النظام المتقدمة. محرك البحث جوجل يمكنه أن يكشف لك عن تقارير من قبل أفراد الأمن التي تكشف العلامات التجارية لجدران الحماية (***firewall***) أو برامج مكافحة الفيروسات المستخدمة في المنظمات الهدف. في بعض الأحيان يوفر لك مخططات الشبكة التي يمكن عن طريقها توجيه الهجوم.

ما هو محرك البحث؟

محرك البحث (الباحوث) هو برنامج حاسوبي مصمم للمساعدة في العثور على مستندات مخزنة على شبكات المعلومات (شبكة الانترنت) أو على حاسوب شخصي. بنيت محركات البحث الأولى اعتمادا على التقنيات المستعملة في إدارة المكتبات الكلاسيكية. حيث يتم بناء فهارس للمستندات تشكل قاعدة للبيانات تفيد في البحث عن أي معلومة. يسمح محرك البحث للمستخدم أن يطلب المحتوى الذي يقابل معايير محددة (والقاعدة فيها تلك التي تحتوي على كلمة أو عبارة ما) ويستدعي قائمةً بالمراجع توافق تلك المعايير. تستخدم محركات البحث مؤشرات/فهارس/مسارد منتظمة التحديث لتشتغل بسرعة وفعالية.

تعرض النتائج على شكل قائمة بعناوين المستندات التي توافق الطلب. يرفق بالعناوين في الغالب مختصر عن المستند المشار إليه أو مقتطف منه للدالة على موافقته للبحث. عناصر قائمة البحث ترتب على حسب معايير خاصة (قد تختلف من محرك لآخر) من أهمها مدى موافقة كل عنصر للطلب.

عند الحديث عن محركات البحث فغالبا ما يقصد محركات البحث على شبكة الإنترنت ومحركات الوِيب بالخصوص. محركات البحث في الويب تبحث عن المعلومات على الشبكة العنكبوتية العالمية، ومنها يستعمل على نطاق ضيق يشمل البحث داخل الشبكات المحلية للمؤسسات أي إنترانت .أما محركات البحث الشخصية فتبحث في الحواسيب الشخصية الفردية.

بعض محركات البحث أيضاً تحفر في البيانات المتاحة على المجموعات الإخبارية، وقواعد البيانات الضخمة، أو أدلة مواقع الوِب. تشتغل محركات البحث عن طريق الخوارزميات، على عكس أدلة المواقع، والتي يقوم عليها محررون بشر.

مما يتكون محرك البحث؟

نجد ان محرك البحث يتكون من ثلاث أشياء اساسيه كالاتى:

- **برنامج العنكبوت(crawler/spider/robot)**

تَستخدِم محركاتُ البحث برنامجَ العنكبوت (**spider**) لإيجاد صفحات جديدة على الويب لإضافتها، ويسمى هذا البرنامج أيضاً الزاحف (**crawler**)لأنه يُبحر في الإنترنت بهدوء لزيارة صفحات الويب والاطلاع على محتوياتها، ويأخذ هذا البرنامج مؤشرات المواقع من عنوان الصفحة(**title**) ، والكلمات المفتاحية (**keywords**) التي تحويها، إضافة إلي محتويات محدِّدات الميتا (**Meta tags**) فيها. ولا تقتصر زيارة برنامج العنكبوت على الصفحة الأولى للموقع بل يتابع البرنامج تَعقُّبَ الروابط (**links**) الموجودة فيها لزيارة صفحات أخرى. أما الغاية من هذه الزيارات فهي وضع النصوص المنتقاة في نظام الفهارس لمحرك البحث، ليتمكن المحرك من العودة إليها فيما بعد، ولم تغب فكرة تغير المحتوى في الموقع عن بال مصممي محرك البحث، إذ ينظم محرك البحث زيارات دورية للمواقع الموجودة في الفهرس للتأكد من التعديلات التي تصيب المواقع المفهرسة.

- **برنامج المُفهرس**

يُمثل برنامج المُفَهرِس(**index program**) ، الكتالوج أحياناً، قاعدة بيانات ضخمة تُوَصِّف صفحات الويب، وتَعتمد في هذا التوصيف على المعلومات التي حَصَلَت عليها من برنامج العنكبوت (**spider**) كما تعتمد على بعض المعايير مثل الكلمات الأكثر تكراراً من غيرها، وتختلف محركات البحث عن بعضها في هذه المعايير، إضافة إلي اختلافها في خوارزميات المطابقة(**ranking algorithms**) .

- **برنامج محرك البحث**

يبدأ دور برنامج محرك البحث عند كتابة كلمة مفتاحية (**keyword**) في مربع البحث (**search box**)؛ إذ يأخذ هذا البرنامج الكلمة المفتاحية ويبحث عن صفحات الويب التي تحقق الاستعلام الذي كونه برنامج المُفهرس في قاعدة بيانات الفهرس (**index database**)، ثم تُعرَض نتيجة البحث المتمثلة بصفحات الويب التي طلبها المُستخدِم في نافذة المُستعرض (**browser window**).

مثال على محركات البحث ما يلي:

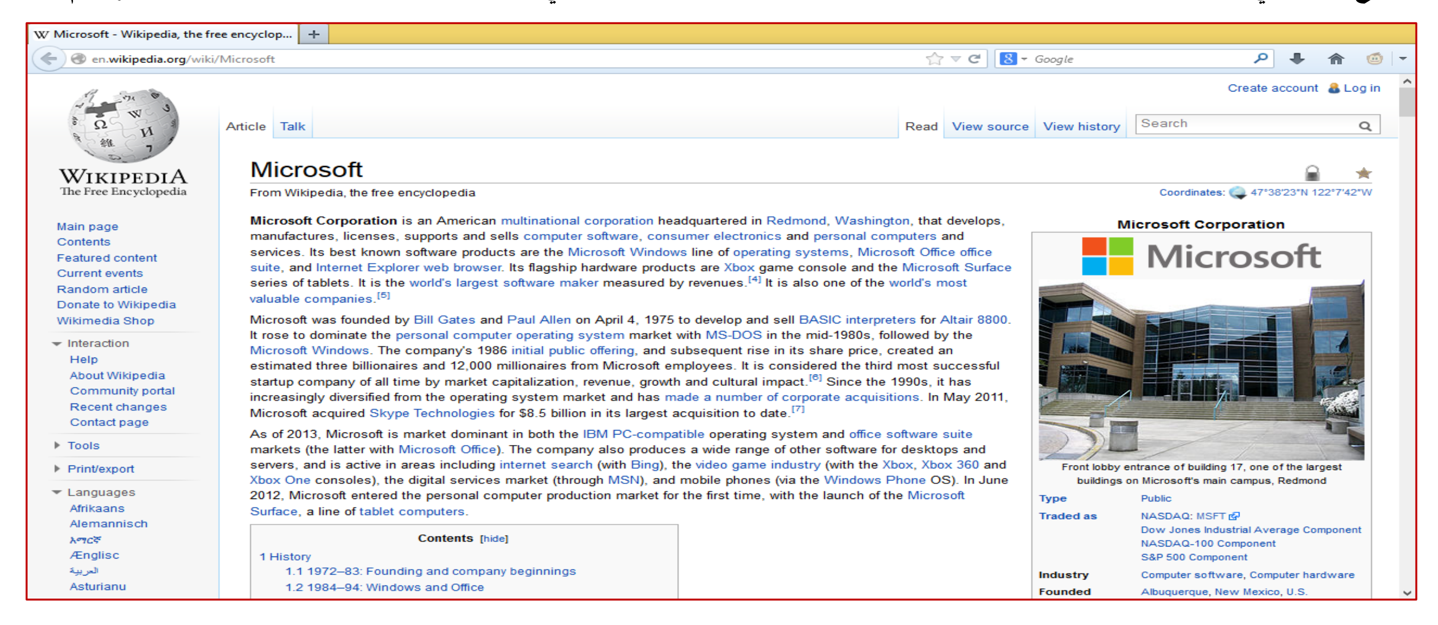
www.google.com – www.yahoo.com – www.bing.com

الموقع التالي يحتوي على قائمه بجميع محركات البحث كالاتى:

http://en.wikipedia.org/wiki/List_of_search_engines

إذا كنت تريد أن تقوم بعملية استطلاع (Footprint) عن المنظمة المستهدفة، على سبيل المثال(XYZ pvt ltd) ، فقم بكتابة هذا (XYZ pvt ltd) في مربع البحث في محرك البحث ثم اضغط على**Enter** . فهذا سوف يقوم بعرض جميع نتائج البحث التي تحتوي على الكلمات الرئيسية(XYZ pvt ltd) . يمكنك أيضا تضييق النتائج بإضافة كلمة محددة أثناء البحث. وعلاوة على ذلك، سوف نناقش تقنيات Footprintingأخرى مثل Website Footprinting و Email Footprinting.

على سبيل المثال، بالنظر في المنظمات، وربما مايكروسوفت. قم بكتابة Microsoft في مربع البحث لمحرك البحث واضغط على Enter، فأن هذا سيتم عرض جميع النتائج التي تحتوي على معلومات حول مايكروسوفت. تصفح النتائج قد يوفر معلومات حاسمة مثل الموقع الجغرافي، عناوين الاتصال، والخدمات المقدمة، وعدد الموظفين، وهكذا. والتي قد تكون مصدرا قيما لبناء استراتيجية الهجوم.



باعتبارك هاكر أخلاقي، إذا وجدت أي من المعلومات الحساسة للشركة الخاصة بك في صفحات نتائج البحث، فإنه يجب عليك إزالة تلك المعلومات. وعلى الرغم من إنك قمت بإزالة هذه المعلومات الحساسة، فإنها قد تكون لا تزال متاحة في ذاكرة التخزين المؤقت لمحرك البحث. لذلك، يجب عليك أيضا التحقق من ذاكرة التخزين المؤقت الخاصة بمحرك البحث للتأكد من أنه تم إزالة البيانات الحساسة بشكل دائم.

إيجاد عناوين URL للشركة خارجيا وداخليا FINDING COMPANY'S EXTERNAL AND INTERNAL URLS

عناوين URL للشركة خارجيا وداخليا توفر الكثير من المعلومات المفيدة إلى المهاجم. هذه العناوين تصف الشركة وتقدم تفاصيل عنها مثل مهمة الشركة ورؤية الشركة، وتاريخ ومنتجات الشركة أو الخدمات التي تقدمها، وما إلى ذلك.
عناوين **URL** التي يتم استخدامها خارج شبكة الشركة للوصول إلى خادم الشركة عبر جدار الحماية تسمى عنوان **URL** الخارجي (**External URL**). هذه العناوين تعمل على الربط المباشر إلى صفحة الويب الخارجية للشركة. يمكنك تحديد URL الخارجي للشركة المستهدفة مع مساعدة من محركات البحث مثل غوغل أو بنج (google or Bing).

إذا كنت ترغب في العثور على عناوين URL الخارجية للشركة، اتبع الخطوات التالية:

1. افتح أي من محركات البحث، مثل غوغل أو بنج.
2. اكتب اسم الشركة المستهدفة في مربع البحث واضغط على Enter .

يتم استخدام عناوين **URL** الداخلية للوصول إلى خادم الشركة مباشرة داخل شبكة الشركات. عنوان **URL** الداخلي يساعد على الوصول إلى الوظائف الداخلية للشركة. معظم الشركات تستخدم أشكال مشتركة لعناوين المواقع الداخلية. لذا، إذا كنت تعرف عنوان **URL** الخارجي

للشركة، فأنه يمكنك التنبؤ بعنوان **URL** الداخلي من خلال التجربة والخطأ. توفر هذه العناوين الداخلية نظرة ثاقبة عن مختلف الإدارات ووحدات الأعمال في المؤسسة. يمكنك أيضا العثور على عناوين المواقع الداخلية للمنظمة الهدف باستخدام أدوات مثل**NetCraft**.



أدوات البحث عن عناوين المواقع الداخلية كالاتى:

- **NetCraft**

المصدر: http://news.netcraft.com

نيتكرافت يتعامل مع خادم الويب، مواقع استضافة تحليل حصة السوق، والكشف عن نظام التشغيل. ويوفر شريط أدوات مجاني لمكافحة الاحتيال (**Net craft toolbar**) / (**anti-phishing toolbar**) لفايرفوكس وكذلك متصفحات الإنترنت إكسبلورر. شريط أدوات نيتكرافت يتجنب هجمات لتصيد المعلومات، ويحمي مستخدمي الإنترنت من المحتالين. فإنه يتحقق من معدل المخاطر وأيضا من موقع استضافة المواقع التي نزورها.

- **Link Extractor**

المصدر: http://www.webmaster-a.com/link-extractor-internal.php

Link Extractor هي أداة استخراج الروابط (**links**) التي تسمح لك أن تختار بين عناوين **URL** الداخلية والخارجية، ثم تعود لك بقائمة من العناوين المرتبطة في صورة **URL** أو قائمة **HTML**. يمكنك استخدام هذه الأداة المساعدة في المواقع المنافسة.

مثال على ذلك مواقع URL الداخلية لمايكروسوفت كالاتى:

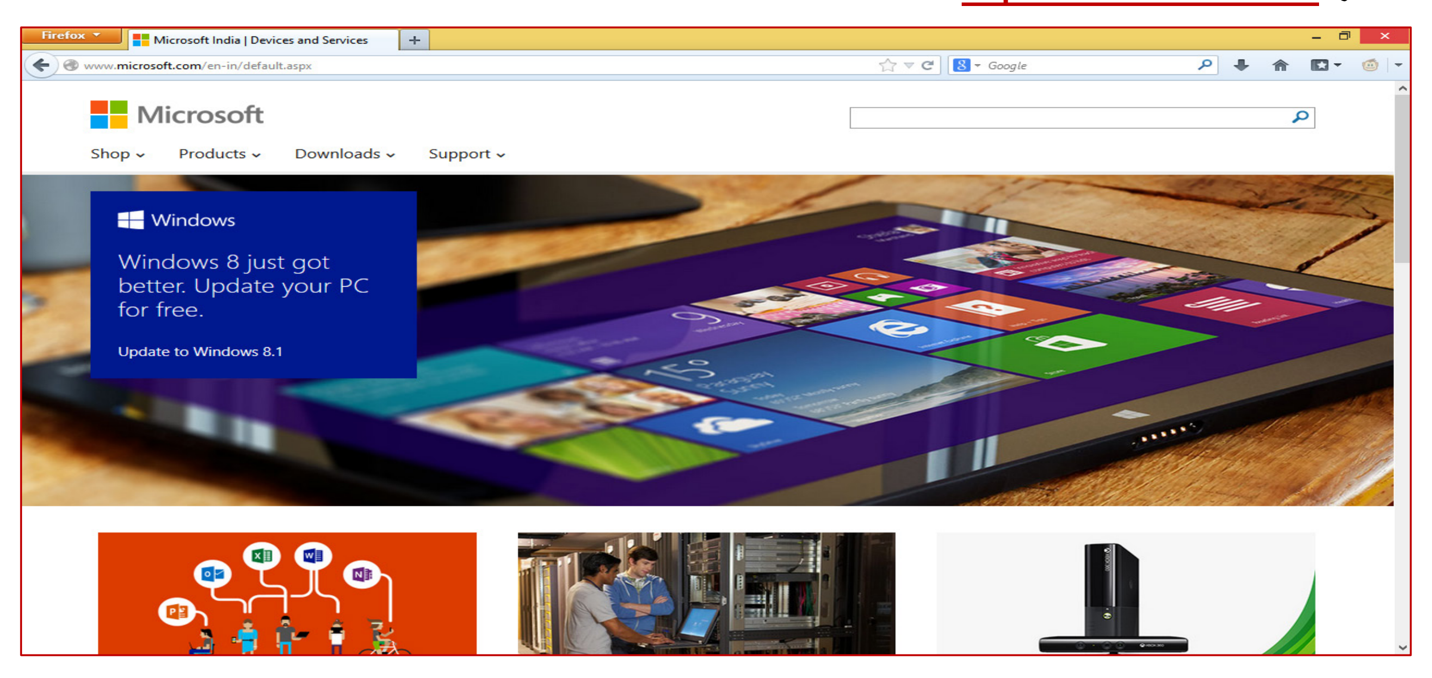


المواقع العامة والمقيدة (PUBLIC AND RESTRICTED WEBSITES)

الموقع العام (Public website) هو موقع مصمم لإظهار وجود المنظمة على شبكة الإنترنت. أنها مصممة لجذب العملاء والشركاء. أنها تحتوي على معلومات مثل تاريخ الشركة والخدمات والمنتجات، ومعلومات الاتصال للمنظمة.

الصورة التالية هي مثال على موقع على شبكة الإنترنت العامة:

المصدر: http://www.microsoft.com



الموقع المقيد (restricted website) هو موقع على شبكة الإنترنت التي تتوفر لعدد قليل من الناس. هؤلاء الناس قد يكونوا العاملين في المؤسسة، أو أعضاء قسم ما، وهكذا. القيود (restriction)يمكن تطبيقها على أساس رقم IP، الدومين أو الشبكة الفرعية **subnet**، واسم المستخدم، وكلمة المرور.

المواقع الخاصة أو المقيدة لمايكروسوفت تشمل الاتي:

http://technet.microsoft.com - http://windows.microsoft.com - http://office.microsoftcom
http://answers.microsoft.com

جمع معلومات عن الموقع الجغرافي COLLECT LOCATION INFORMATION

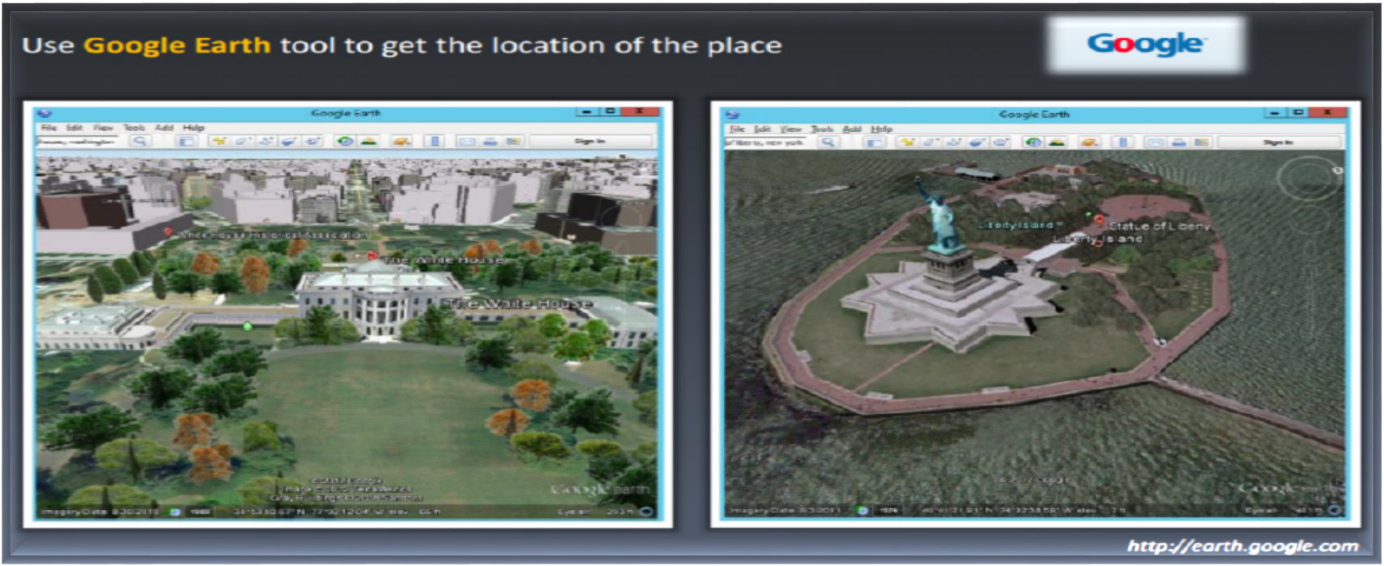
معلومات مثل الموقع الجغرافي للمنظمة تلعب دورا حيويا في عملية القرصنة. ويمكن الحصول على هذه المعلومات باستخدام تقنية **Footprinting**. بالإضافة إلى الموقع الجغرافي، فإنه يمكننا أيضا جمع المعلومات مثل شبكة الواي فاي المحيطة (Wi-Fi hotspots) التي قد تكون وسيلة لاختراق شبكة المنظمة الهدف.

المهاجمين مع العلم بموقع المنظمة الهدف قد يحاولون التفتيش في قمامة هذه المنظمة، والمراقبة، الهندسة الاجتماعية، والهجمات غير الفنية الأخرى لجمع المزيد من المعلومات عن المنظمة المستهدفة. وبمجرد معرفة موقع الهدف، فإن صور الأقمار الصناعية المفصلة

للموقع يمكن الحصول عليها باستخدام مصادر مختلفة متاحة على شبكة الإنترنت مثل **http://www.google.com/earth** و **https://maps.google.com**. حيث يمكن استخدام هذه المعلومات من قبل القراصنة للوصول الغير مصرح به إلى المباني والشبكات السلكية واللاسلكية، والنظم، وهلم جرا.

مثال: earth.google.com

جوجل ايرث هو أداة قيمة للقراصنة التي تسمح لك بإيجاد المكان، والإشارة إليه، والتكبير في هذا الموقع لاستكشاف. يمكنك حتى الوصول إلى صور **3D** التي تصور معظم الأرض بتفاصيل عالية الجودة.





مثال: maps.google.com

يوفر خرائط جوجل ميزة عرض (**View**)الشوارع التي توفر لك مجموعة من الصور عن المبنى، وكذلك المناطق المحيطة بها، بما في ذلك شبكات الواي فاي. يستخدم المهاجمون خرائط **Google** للعثور على أو تحديد مداخل المباني، الكاميرات الأمنية، البوابات، أماكن الاختباء، نقاط الضعف في الأسوار المحيطة، الموارد ذات الفائدة مثل الاتصالات الكهربائية، لقياس المسافة بين الأهداف المختلفة، وهكذا.

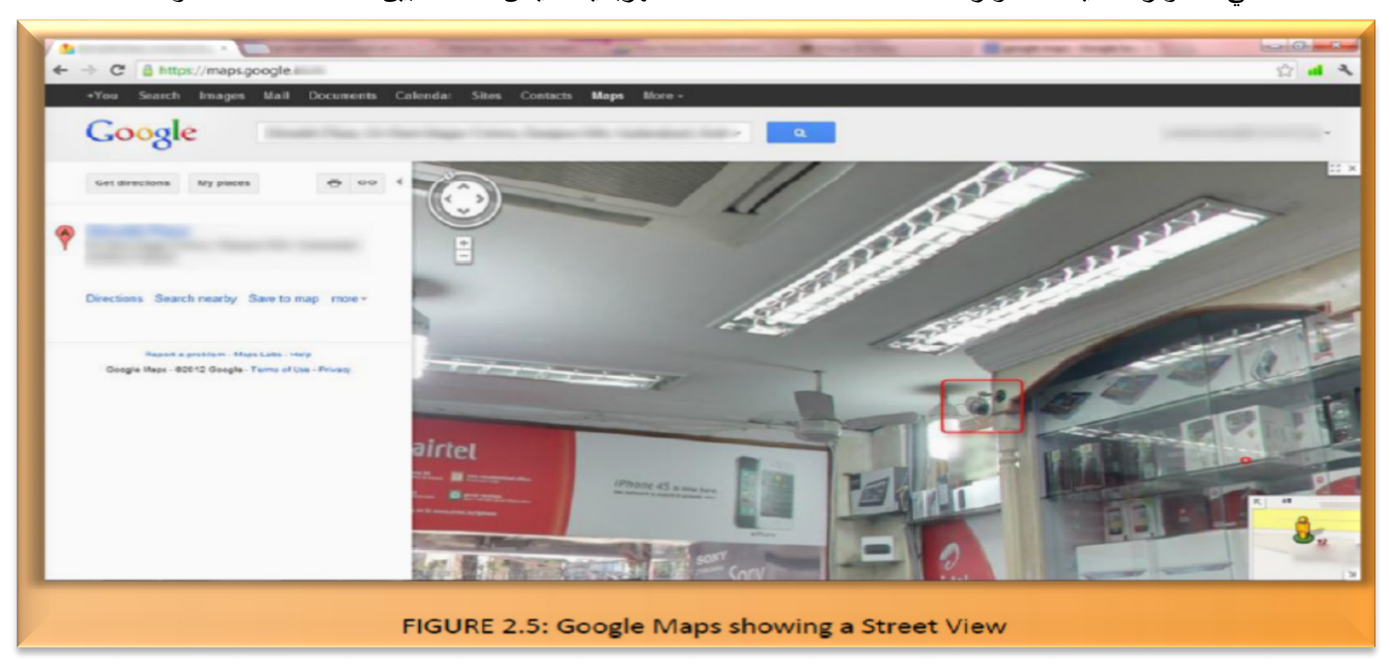


FIGURE 2.5: Google Maps showing a Street View

البحث عن الناس PEOPLE SEARCH

يمكنك استخدام مواقع السجل العام للعثور على معلومات حول عناوين البريد الإلكتروني للأشخاص وأرقام الهواتف وعناوين المنازل، وغيرها من المعلومات. باستخدام هذه المعلومات يمكنك المحاولة للحصول على التفاصيل المصرفية وتفاصيل بطاقة الائتمان، وأرقام الهواتف النقالة، والتاريخ الماضي، وما إلى ذلك. هناك العديد من خدمات البحث عن الأشخاص المتاحة في الإنترنت التي تساعدك في إيجاد الناس. http://pipl.com و http://www.spokeo.com أمثلة على خدمات البحث عن الأشخاص التي تسمح لك بالبحث عن الأشخاص باستخدام الاسم، والبريد الإلكتروني، واسم المستخدم، والهاتف، أو عنوان.

خدمات البحث عن الأشخاص قد توفر لك بعض المعلومات مثل الاتي:

1. عنوان السكن وعنوان البريد الإلكتروني.
2. أرقام الاتصال وتاريخ الميلاد.
3. صور والملف الخاص به في الشبكات الاجتماعية.
4. عناوين المدونة الخاصة به (Blog URLs).
5. صور الأقمار الصناعية من المساكن الخاصة.

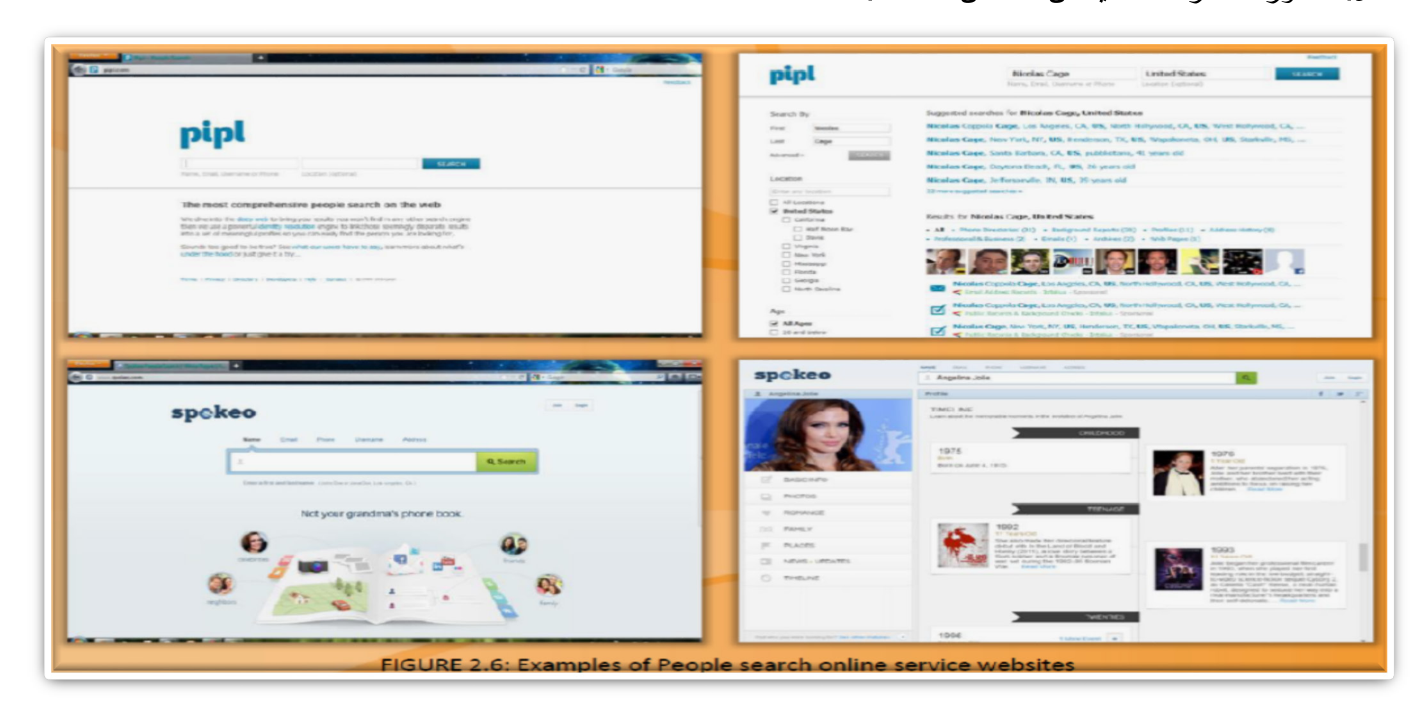
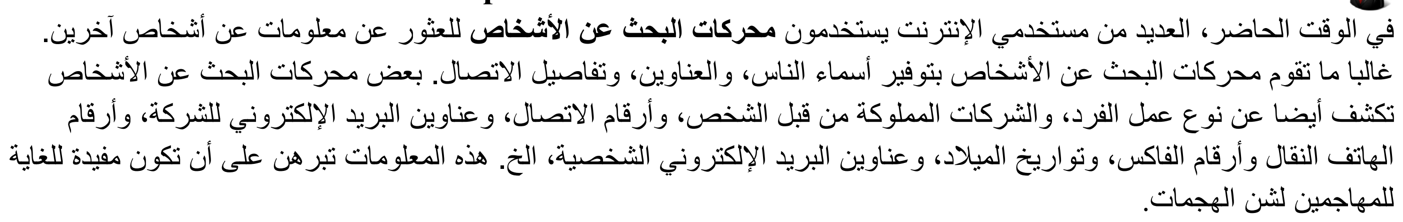


FIGURE 2.6: Examples of People search online service websites

خدمات البحث عن الأشخاص أونلاين People Search Online Services



في الوقت الحاضر، العديد من مستخدمي الإنترنت يستخدمون **محركات البحث عن الأشخاص** للعثور عن معلومات عن أشخاص آخرين. غالبا ما تقوم محركات البحث عن الأشخاص بتوفير أسماء الناس، والعناوين، وتفاصيل الاتصال. بعض محركات البحث عن الأشخاص تكشف أيضا عن نوع عمل الفرد، والشركات المملوكة من قبل الشخص، وأرقام الاتصال، وعناوين البريد الإلكتروني للشركة، وأرقام الهاتف النقال وأرقام الفاكس، وتواريخ الميلاد، وعناوين البريد الإلكتروني الشخصية، الخ. هذه المعلومات تبرهن على أن تكون مفيدة للغاية للمهاجمين لشن الهجمات.

- **بعض من محركات البحث عن الأشخاص كالاتى:**

ZABA®SEARCH

المصدر: http://www.zabasearch.com

Zaba Search هو محرك بحث عن الاشخاص التي توفر المعلومات مثل العنوان ورقم الهاتف والموقع الحالي، وما إلى ذلك من الناس في الولايات المتحدة. فإنه يسمح لك للبحث عن الناس باستخدام أسمائهم.



المصدر: http://www.zoominfo.com

ZoomInfo هو دليل استخدام رجال الأعمال والتي يمكنك أن تجد الاتصالات التجارية ، وملامح الناس المهنية ، والسير الذاتية ، وتاريخها العملي ، والانتماءات ، ووصلات لملفات الموظف مع معلومات الاتصال التحقق ، و أكثر من ذلك.



المصدر: http://wink.com

Wink People Search هو محرك بحث عن الأشخاص التي توفر معلومات عن الأشخاص بالاسم والموقع. أنه يعطي رقم الهاتف والعنوان، والمواقع، والصور، العمل، المدرسة، الخ.



المصدر: http://www.anywho.com

Any who هو موقع يساعدك في العثور على معلومات عن الأشخاص والشركات الخاصة بهم ، ومواقعها على الإنترنت. مع مساعدة من رقم الهاتف، يمكنك الحصول على جميع التفاصيل للفرد.



المصدر: https://www.peoplelookup.com

People Lookup هو محرك بحث عن الأشخاص التي تسمح لك بالعثور على الأشخاص، ومواقعهم، ومن ثم التواصل معهم. كما أنه يسمح لك بالبحث عن رقم هاتف، البحث عن أرقام الهواتف المحمولة، العثور على عنوان أو رقم الهاتف، البحث عن الأشخاص في الولايات المتحدة. يستخدم قاعدة بيانات هذه المعلومات من السجلات العامة.



المصدر: http://www.123people.com

123 People Search هي أداة بحث عن الأشخاص التي تسمح لك بالعثور على المعلومات مثل السجلات العامة ، وأرقام الهواتف والعناوين و الصور، والفيديو ، و عناوين البريد الإلكتروني.

المصدر: http://www.peekyou.com

PeekYou هو محرك بحث عن الأشخاص التي تسمح لك بالبحث عن ملامح ومعلومات عن الأشخاص في الهند وبعض المدن الكبرى المكتظة بالموظفين والمدارس. فإنه يسمح لك للبحث عن الأشخاص بأسمائهم أو أسماء المستخدمين.



المصدر: http://www.intelius.com

Intelius هو ملفات سجلات عامة التي تقدم خدمة المعلومات. فإنه يسمح لك بالبحث عن الأشخاص في الولايات المتحدة عن طريق الاسم والعنوان والهاتف، أو البريد الإلكتروني.

المصدر: http://www.peoplesmart.com

PeopleSmart عبارة عن خدمة بحث عن الأشخاص. تسمح لك بالعثور على المعلومات عن الاشخاص مع اسمائهم، المدينة، الدولة. بالإضافة إلى ذلك، فإنه يسمح لك لتنفيذ عمليات البحث العكسي للهاتف، بحث البريد الإلكتروني، البحث عن طريق العنوان، والبحث الإقليمي.



المصدر: http://www.whitepages.com

WhitePages هو محرك بحثى عن الأشخاص. يعمل على تزويدك بكثير من المعلومات عن الأشخاص عن طريق أسمائهم وأماكنهم. باستخدام أرقام التليفونات يمكنك إيجاد عنوان الشخص.



عملية البحث عن الأشخاص في الشبكات الاجتماعية People Search on Social Networking Services

البحث عن الأشخاص على مواقع الشبكات الاجتماعية تتميز بالسهولة واليسر. خدمات الشبكات الاجتماعية هي خدمات أونلاين، أو منصات، أو مواقع تركز على تسهيل بناء الشبكات الاجتماعية أو العلاقات الاجتماعية بين الناس. توفر هذه المواقع المعلومات التي يتم توفيرها من قبل المستخدمين. هنا الناس سواء بصورة مباشرة أو غير مباشرة مرتبطين مع بعضهم البعض عن طريق الاهتمام المشترك، أو نفس مكان العمل، أو المجتمعات التعليمية، الخ

مواقع الشبكات الاجتماعية تسمح للناس لتبادل المعلومات بسرعة وفعالية كما يتم تحديث هذه المواقع في الوقت الحقيقي. لأنها تتيح استكمال الحقائق حول الأحداث القادمة أو الحالية، والإعلانات والدعوات، وهكذا. وبالتالي، فإن مواقع الشبكات الاجتماعية يعتبر منصة كبيرة للبحث عن الأشخاص والمعلومات المتعلقة بهم. من خلال البحث عن الأشخاص على خدمات الشبكات الاجتماعية، فانه يمكنك جمع المعلومات الهامة التي من شأنها أن تكون مفيدة في أداء الهندسة الاجتماعية أو أنواع أخرى من الهجمات.

العديد من مواقع الشبكات الاجتماعية تسمح للزوار للبحث عن أشخاص من دون تسجيل، وهذا يجعل البحث عن الأشخاص على مواقع الشبكات الاجتماعية مهمة سهلة بالنسبة لك. يمكنك البحث باستخدام اسم الشخص، والبريد الإلكتروني، أو العنوان. بعض المواقع تسمح لك للتحقق ما إذا كان الحساب هو حاليا قيد الاستخدام أم لا. هذا يسمح لك للتحقق من حالة الشخص الذي تبحث عنه.

__فيما يلي قائمة بأهم مواقع الشبكة الاجتماعية كالاتى:__



Facebook

المصدر: https://www.facebook.com

الفاسبوك يسمح لك بالبحث عن الأشخاص، وأصدقائهم، وزملائهم والأشخاص الذين يعيشون حولهم والأخرين الذين كانوا ينتمون لهم. بالإضافة إلى ذلك يمكن أيضا إيجاد المعلومات الشخصية عن الشخص الهدف مثل الشركة التي يعمل بها وماذا يعمل والمكان الذي يعيش فيه حاليا وأرقام التليفونات والبريد الإلكتروني وبعض الصور الشخصية وبعض الفيديوهات وهكذا. الفاسبوك يمكنك من البحث عن الأشخاص باستخدام أسمائهم أو البريد الإلكتروني الذي يخصهم.

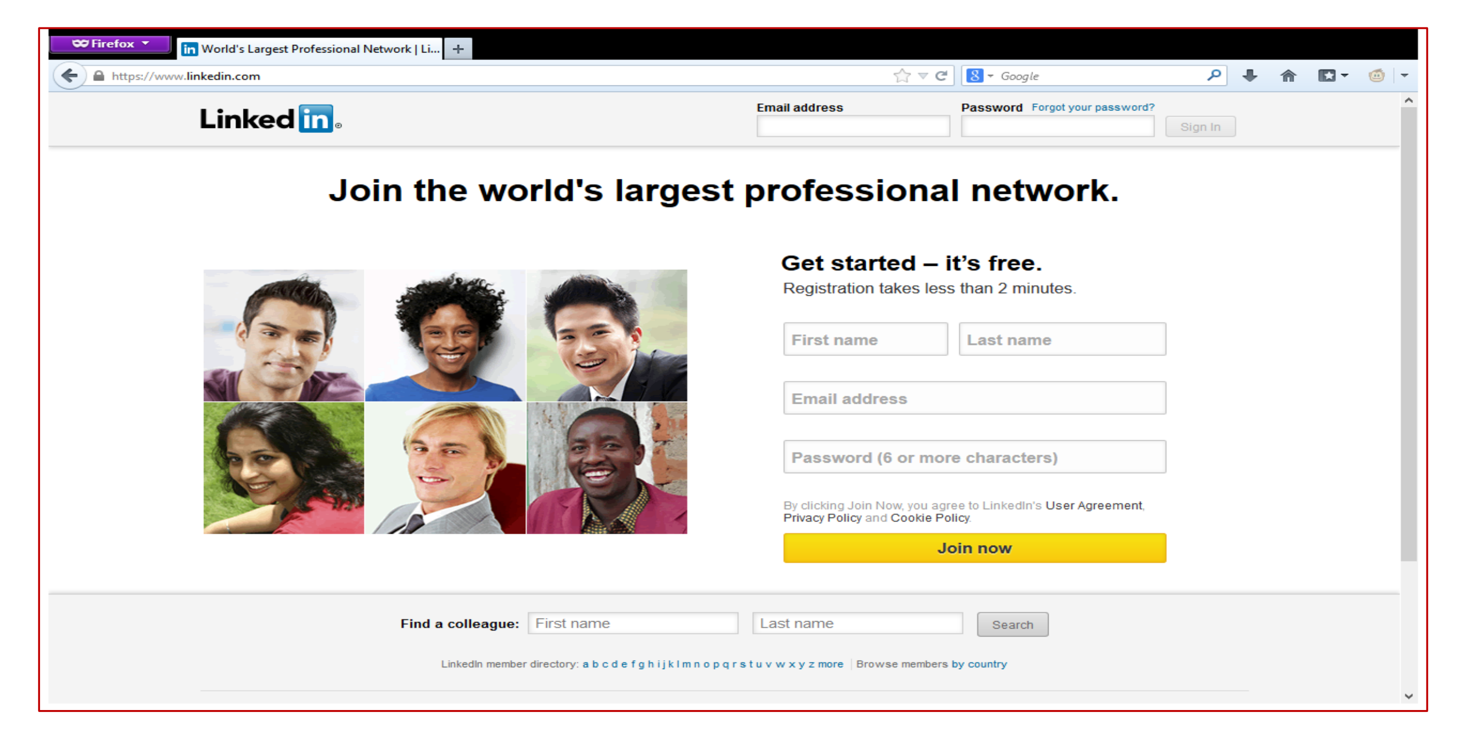




LinkedIn

المصدر: https://www.linkedin.com

هو عباره عن موقع للتواصل الاجتماعي للأشخاص المحترفين حيث يسمح لك بإيجاد الأشخاص عن طريق الاسم، بعض الكلمات، الشركة التي يعمل بها، اسم المدرسة وهكذا. البحث عن الأشخاص في **LinkedIn** يعطيك الكثير من المعلومات مثل الاسم، التعين، اسم الشركة التي يعمل بها، موقع الشخص الحالي، والدرجة التعليمية ولكن لكي تستخدم **LinkedIn** يجب أن تكون مسجلا فيه.





Twitter

المصدر: https:// twitter.com

هو عباره عن شبكه اجتماعيه التي تسمح بإرسال رسائل نصيه للقراءة وتسمى تويت tweets. حتى الأشخاص غير مسجلين يمكنهم قراءة هذه الرسائل.



Google+

المصدر: https://plus.google.com

هو موقع تواصل اجتماعي يهدف إلى جعل عملية المشاركة على الموقع يشبه كثيرا المشاركة في الحياة الحقيقية. من خلال هذا الموقع يمكن جمع المعلومات المهمة عن المستخدمين واستخدام هذه المعلومات للقرصنة على أنظمة تشغيلهم.



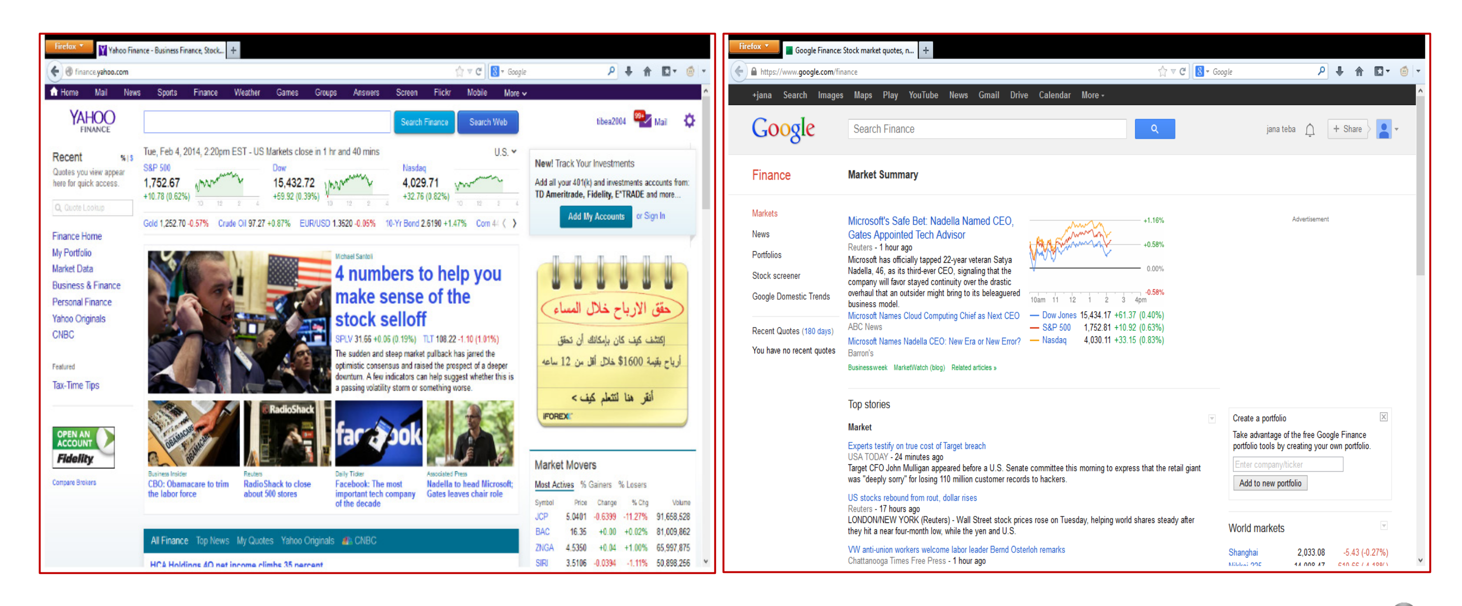
جمع المعلومات باستخدام الخدمات المالية GATHER INFORMATION FROM FINANCIAL SERVICES

الخدمات المالية (**Financial services**) مثل **Google Finance**، **Yahoo! Finance**، والتي توفر الكثير من المعلومات المفيدة مثل القيمة السوقية لأسهم الشركة، نبذة عن الشركة وبعض التفاصيل الأخرى عن المنافسين، وهكذا. هذه المعلومات تختلف من سيرفر إلى أخر. من أجل الاستفادة من هذه الخدمات مثل تنبيهات البريد الإلكتروني وتنبيهات الهاتف، فإن المستخدمون يحتاجون للتسجيل في الخدمات المالية. وهذا يعطي فرصة للمهاجمين لانتزاع معلومات مفيدة لعملية القرصنة.

العديد من الشركات المالية تعتمد على الوصول إلى شبكة الإنترنت، وأداء المعاملات، ووصول المستخدمين إلى حساباتهم. القراصنة يمكنهم الحصول على معلومات حساسة وخاصة من المستخدمين عن طريق سرقة المعلومات، **key loggers**، وهكذا. المهاجمون أيضا يمكنهم الاستيلاء على هذه المعلومات من خلال تنفيذ جرائم الإنترنت، واستغلال ذلك من خلال المساعدة من قبل التهديدات الغير ضعيفة (تصميم برمجيات على سبيل المثال؛ تعمل على كسر آلية المصادقة).

وفيما يلي بعض من التهديدات الغير ضعيفة(non-vulnerable threats)

- فيضانات الخدمة (Service flooding)
- هجوم القوة الغاشمة(Brute force attack)
- الخداع(Phishing)



عمليات الاستطلاع باستخدام مواقع البحث عن العمل FOOTPRINTING THROUGH JOB SITES

المهاجمين يمكنهم جمع المعلومات القيمة مثل نظام التشغيل، إصدارات البرامج وتفاصيل البنية التحتية للشركة، ومخطط قاعدة البيانات للمنظمة، وذلك من خلال ***Footprinting*** لمواقع العمل المختلفة باستخدام تقنيات مختلفة. تبعا لمتطلبات النشر لفرص العمل، فإن المهاجمين يكونوا قادرين على دراسة الأجهزة والمعلومات المتعلقة بالشبكة، والتقنيات المستخدمة من قبل الشركة. معظم مواقع الشركة لديها قائمة من الموظفين الرئيسيين مع عناوين بريدهم الإلكتروني. هذه المعلومات قد تكون مفيدة للمهاجمين. على سبيل المثال، إذا كانت الشركة تريد استئجار شخص لوظيفة إدارة الشبكة، فإنه تعمل على نشر متطلبات العمل المتعلقة بوظيفة إدارة الشبكات.

باستخدام مواقع البحث عن عمل (Footprinting through job sites) فان المهاجمين يمكنهم الحصول على المعلومات الأتية:

متطلبات العمل – ملفات الموظفين – معلومات عن الأجهزة لديهم – معلومات عن التطبيقات لديهم.

فيما يلي قائمة بمواقع العمل المشهورة:

http://www.monster.com
http://www.careerbuilder.com
http://www.dice.com
http://www.simplyhired.com
http://www.indeed.com
http://www.usajobs.gov

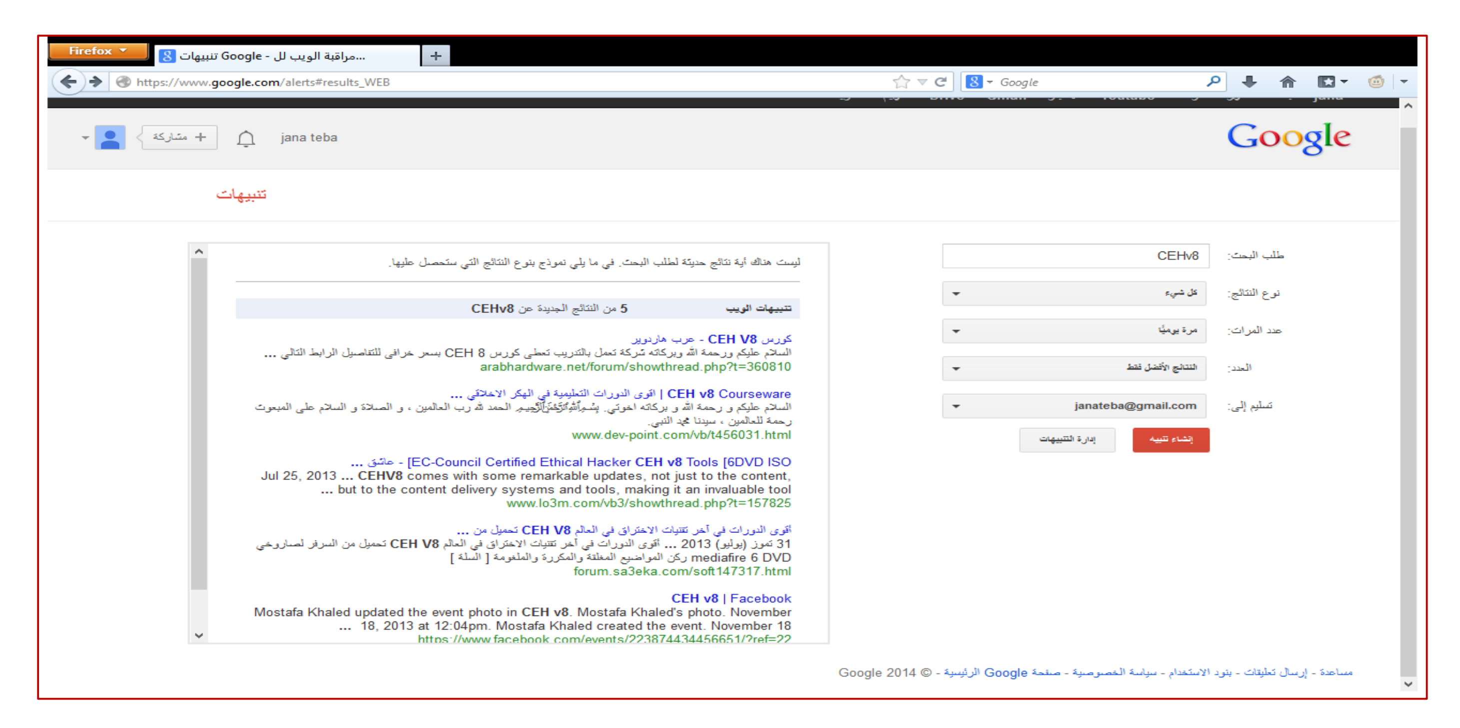
رصد الأهداف عن طريق التنبيهات MONITORING TARGETS USING ALERTS

التنبيهات هي محتوى خدمات الرصد الآلي (**Monitoring services**) والتي تقدم معلومات محدثه إلى تاريخ اليوم على أساس التفضيل الخاص بك، عادة يتم عرض المعلومات عن طريق البريد الإلكتروني أو الرسائل القصيرة. من أجل الحصول على هذه التنبيهات، فإنك تحتاج إلى التسجيل في المواقع، ولكي تقوم بالتسجيل فإنك أيضا تحتاج إلى تسجيل البريد الإلكتروني أو رقم الهاتف الخص بك في الخدمة. هنا يأتي دور القراصنة حيث يمكنهم جمع هذه المعلومات الحساسة من خدمات التنبيه واستخدامها لمزيد من عمليات الهجوم.

Google Alerts

المصدر: https://www.google.com/alerts

تنبيهات جوجل هي محتوى خدمة المراقبة الذي يقوم بطريقه تلقائيه بإعلام المستخدمين عن موضوع معين حسب اختيار المستخدم وذلك عند وجود محتوى جديد من الأخبار، أو على شبكة الإنترنت، أو المدونات (**Blogs**)، والفيديو، و/أو مواضيع للمناقشة من قبل مجموعه تقابل الموضوع الذي يبحث عنه المستخدم ويتم تخزينها بواسطة خدمة تنبيهات جوجل.



بعض مواقع التنبيهات الأخرى كالاتى:

Yahoo! Alerts-1 (**http://alerts.yahoo.com**)

Giga Alert-2 (**http://www.gigaalert.com**)

2-WEBSITE FOOTPRINTING عملية الاستطلاع عن المواقع الإلكترونية

فيما سبق قمنا بشرح أول خطوه في منهجية عملية الاستطلاع (**Footprinting methodology**) من خلال محركات البحث. أما الأن سوف نقوم بشرح عملية الاستطلاع عن المواقع الإلكترونية.

من الممكن أن يقوم المهاجمين ببناء خريطة تفصيلية لبنية ومعمارية الموقع الإلكتروني بدون تشغيل **IDS** أو بدون إثارة أي شكوك من قبل مسئولي الأنظمة(**admin**) . ويمكن تحقيق ذلك إما بمساعدة أدوات متطورة لـ **Footprinting** أو مع الأدوات الأساسية التي تأتي جنبا إلى جنب مع نظام التشغيل، مثل **telnet** و**browser**. باستخدام أداة نيتكرافت (**NetCraft**) يمكنك جمع معلومات عن الموقع مثل عنوان**IP** ، الاسم المسجل وعنوان مالك الدومين، اسم الدومين، المضيف المرتبطين بالموقع (**host of the site**) وتفاصيل نظام التشغيل، وغيرها من المعلومات. ولكن هذه الأداة قد لا تعطي كل هذه التفاصيل عن كل المواقع. في مثل هذه الحالات، يجب تصفح الموقع المستهدف.

تصفح الموقع المستهدف سوف يوفر لك المعلومات التالية:

1) البرمجيات المستخدمة وإصدارها: حيث يمكنك أن تجد ليس فقط البرنامج المستخدمة ولكن أيضا إصدار النسخة بسهولة على الموقع المستندة إلى البرامج الجاهزة.
2) نظام التشغيل المستخدمة: عادة نظام التشغيل يمكن تحديده.
3) المجلدات الفرعية والمعاملات (**sub-directories and parameters**): حيث يمكنك أن تكشف المجلدات الفرعية والمعاملات عن طريق جعل ملاحظة على كافة عناوين المواقع URLs أثناء تصفح الموقع المستهدف.
4) اسم الملف، المسار، أسماء الحقول في قاعدة البيانات، أو استعلام: يجب تحليل أي شيء يشبه اسم الملف، المسار، أسماء الحقول في قاعدة البيانات بعد الاستعلام أو الاستعلام بعناية للتحقق ما إذا كان يوفر فرصا للحقن **SQL injection**.
5) منصة الاسكربات: مع مساعدة من اسم امتداد ملف الاسكريبت مثل (**.php**)، (**.asp**)، (**.jsp**)، الخ. فانه يمكنك بسهولة تحديد منصة الاسكريبت الذي يستخدمه الموقع المستهدف.
6) بيانات الاتصال وتفاصيل **CMS**: عادة ما تقدم صفحات تفاصيل الاتصال بعض المعلومات مثل أسماء وأرقام الهاتف وعناوين البريد الإلكتروني، وموقع المشرف أو مدعمي الناس. يمكنك استخدام هذه التفاصيل لتنفيذ هجوم الهندسة الاجتماعية.

برنامج(CMS): يسمح لعناوين **URL** من إعادة كتابتها من أجل إخفاء أسماء امتدادات ملفات الاسكريبت. في هذه الحالة، تحتاج إلى بذل المزيد من الجهد القليل لتحديد منصة ملف الاسكريبت.

يمكن استخدام كل من (Zaproxy، Owasp، Firebug، Brup Suite، Paros Proxy،etc) لعرض العناوين التي تزودك بالمعلومات التالية:

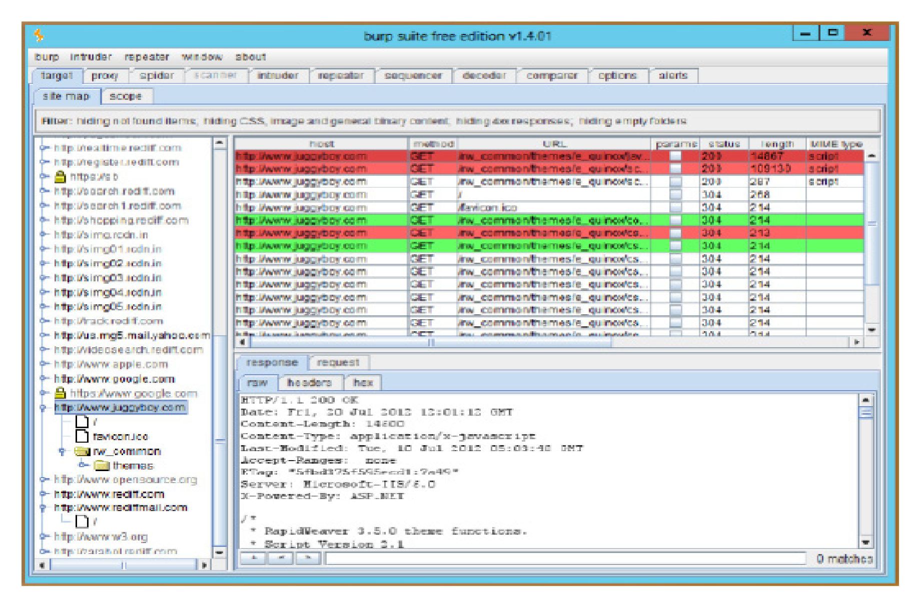
- حالة الاتصال ونوع الاتصال (**connection status and connection-type**)
- النطاقات المقبولة **Accept-ranges**
- المعلومات الأخيرة المعدلة **Last-Modified information**
- **X-Powered-By information**
- خوادم الويب المستخدمة وإصداراتها **Web server in use and its version**



Burp suite

المصدر: **http://portswigger.net**

ملحوظة هذا التطبيق يحتاج إلى منصة الجافا لكي يعمل ويتم إعداده لكي يعمل بالتناوب مع المتصفح الخاص بك ولرؤية طريقة إعداده مع المتصفح الخاص بك فيمكن زيارة موقع هذا التطبيق والذي يوضح طريقة إعداده مع المتصفح وكيفية عمله وفيما يلي screenshot له كالاتى:






Firebug

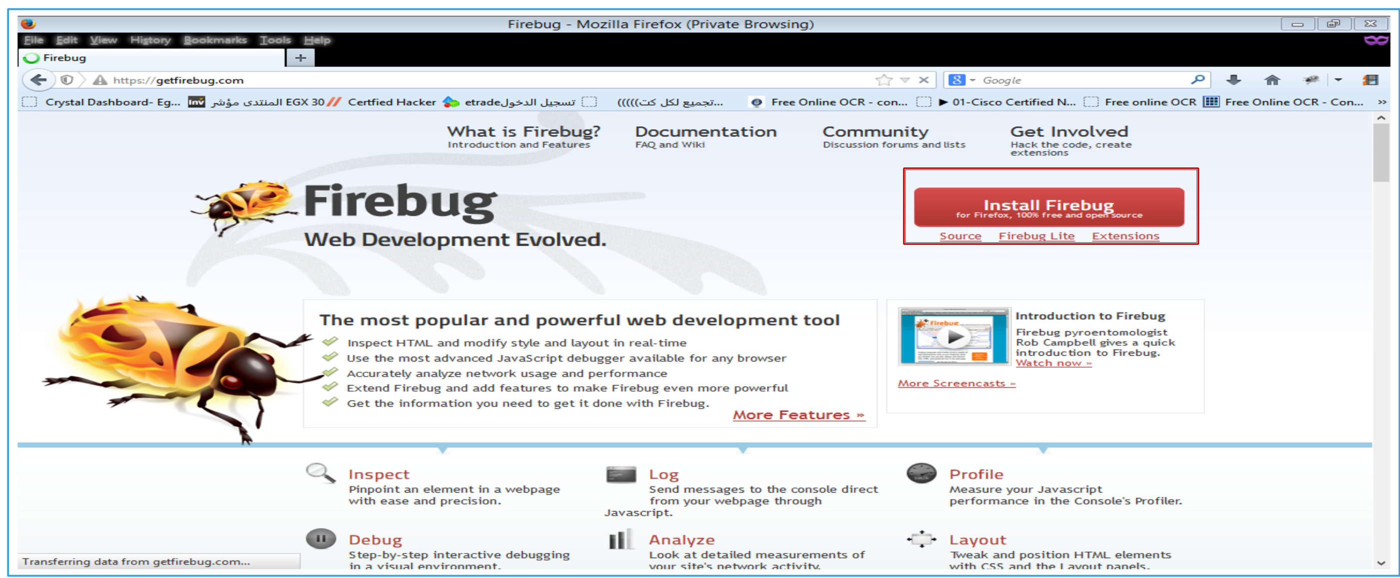
المصدر: **http://getfirebug.com/**

تعمل هذه الأداة مع **متصفح الويب فايرفوكس** تدعمه بمجموعه من أدوات التطوير والتي تمكنه من editing وdebug وmonitor لـ CSS وHTML وJavaScript الموجودة في أي صفحة ويب.

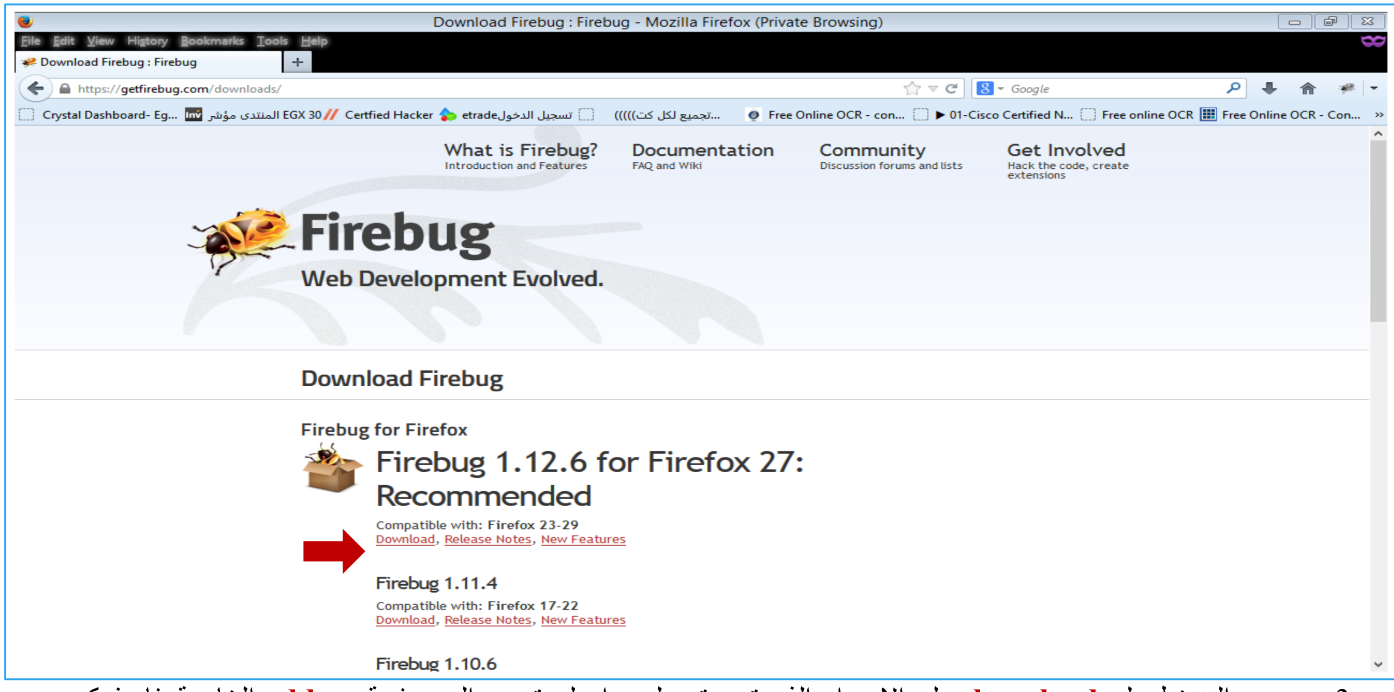
ملحوظة: هذا التطبيق يعمل على جميع أنظمة التشغيل لأنه يعتمد في عمله على متصفح الويب فقط وليس نظام التشغيل.

كما تعلمون جميعا، ان البريد الإلكتروني هو واحد من اهم الأدوات التي تم إنشاؤها. ولكن لسوء الحظ قد يساء استخدامه من قبل المهاجمين عن طريق إرسال رسائل البريد المزعجة (spam emails) وذلك للتواصل سرا وإخفاء أنفسهم وراء هذه الرسائل المزعجة(**spam**)، أثناء محاولته لتفويض بعض التعاملات التجارية. في مثل هذه الحالات، يصبح من الضروري للمهندس المسئول عن اختبار معدلات الامن تتبع البريد الكترونى للعثور على مصدر البريد الإلكتروني وخاصة الذي استخدم في ارتكاب عملية القرصنة باستخدام البريد الإلكتروني. وهذا ما سوف نتطرق اليه لاحقا والذي قد يساعد أيضا في كيفية العثور على الموقع (**location**)عن طريق تتبع البريد الكترونى باستخدام **eMailTrackerPro**والذي يمكنه أيضا توفير بعض معلومات مثل المدينة والولاية والدولة، وما إلى ذلك. غالبية المسئولين عن اختبار الاختراق يستخدموا متصفح موزيلا فايرفوكس كمستعرض ويب لأنشطتهم. هنا سوف نتعلم استخدام **Firebug** لاختبار اختراق تطبيقات الويب وجمع معلومات كاملة.

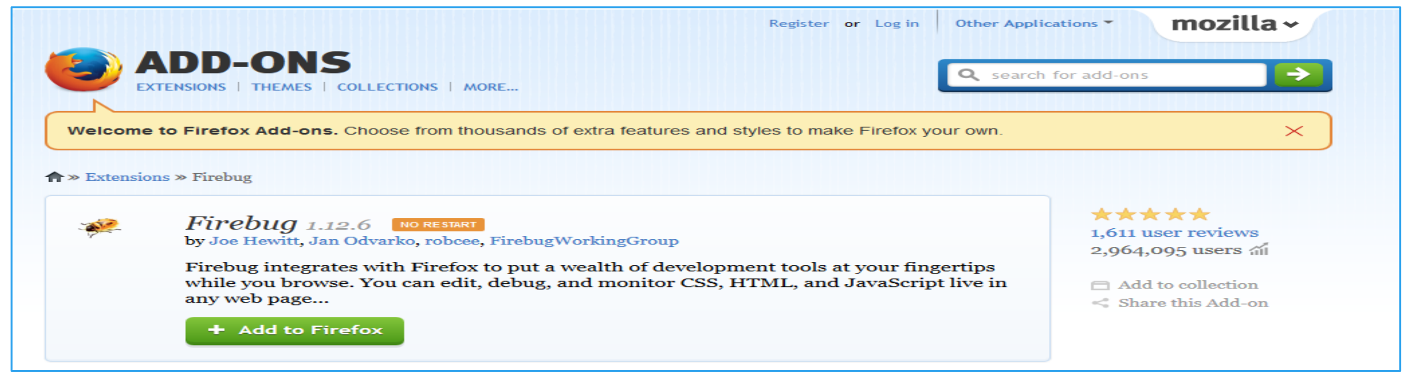
1- أولا نعمل على تحميل هذه الأداة وذلك بفتح متصفح الويب فايرفوكس وذلك لان هذه الأداة لا تعمل الا مع هذا المتصفح فقط ثم نقوم بالذهاب الى الموقع التالي[**https://getfirebug.com**] كالاتى:



2- ثم نختار **Install Firebug** والذي يعمل على توجيهك الى صفحة الويب الذي من خلاله سوف تختار الإصدار الذي يناسبك لتقوم بتحميله كالاتى:



3- بمجرد الضغط على **download** على الإصدار الذي تريد تحميله يبدا على توجيه الى صفحة **add-on** الخاصة بفايرفوكس والذي من خلالها نضغط على **Add to Firefox** ثم تظهر شاشة أخرى نختار **install now** حتى يتم تثبيت التطبيق **Firebug** كالاتى:



4- بعد الانتهاء من التثبيت نلاحظ وجود الأيقونة الخاصة بالـ **Firebug** في الجانب الأيمن من شريط الأدوات باللون الرمادي كالاتى

5- نقوم بالضغط عليها للتحول الى اللون الأصفر وحتى يظهر شريط الأدوات الخاص بها كالاتى:

6- نجد ان شريط الأدوات يحتوي على العديد من الأدوات مثل **Console** و**html** و**CSS** و**script** و**Net** وغيرها.

7- هنا سوف نذهب الى موقع مايكروسوفت [http://www.microsoft.com/ar-EG/default.aspx] ونفعل **Firebug** عليه.

8- **Console panel** يقدم لك سطر الأوامر الخاص بالجافا سكريبت، يسرد كافة أنواع الرسائل ويقدم التعريف لأوامر جافا سكريبت.

9- **HTML panel** تقدم لك صفحة **HTML/XML** الذي تم إنشاؤه من الصفحة المفتوحة حاليا. وهو يختلف عن طريقة العرض التقليدي للـ **source code**، لأنه يعرض أيضا جميع المعالجات على شجرة **DOM**. على الجانب الأيمن فإنه يعرف أنماط **CSS** المحددة حاليا، والأساليب المحسوبة لذلك، ومعلومات التخطيط ومتغيرات **DOM** المسندة إليه انظر الى الشكل السابق او بمعنى اخر ان هذه الـ **panel** تقدم لك بعض المعلومات مثل اكواد الانشاء (**source code**) والعناوين الداخلية (**internal URLs**) وغيرها من المعلومات.

10- **Net panel** الغرض الرئيسي من هذه هو مراقبة حركة المرور لـ **HTTP** التي بدأتها صفحة ويب على شبكة الإنترنت. ببساطة هي تقديم جميع المعلومات التي تم جمعها وتجميعها للمستخدم. ويتكون محتواه من قائمة إدخالات حيث يمثل كل إدخال واحد من الاتي **request** و**respond** و**round trip** التي تم انشائها عن طريق صفحة الويب الهدف.

11- **Cookies Panel** يسمح بعرض ومعالجة ملفات **cookies** التي وضعتها الصفحة الحالية.

يمكن الاطلاع على تفاصيل اكتير وجميع الأوامر المستخدمة لهذه الأداة عن طريق الاطلاع على الصفحة التالية:

https://getfirebug.com/wiki/index.php/

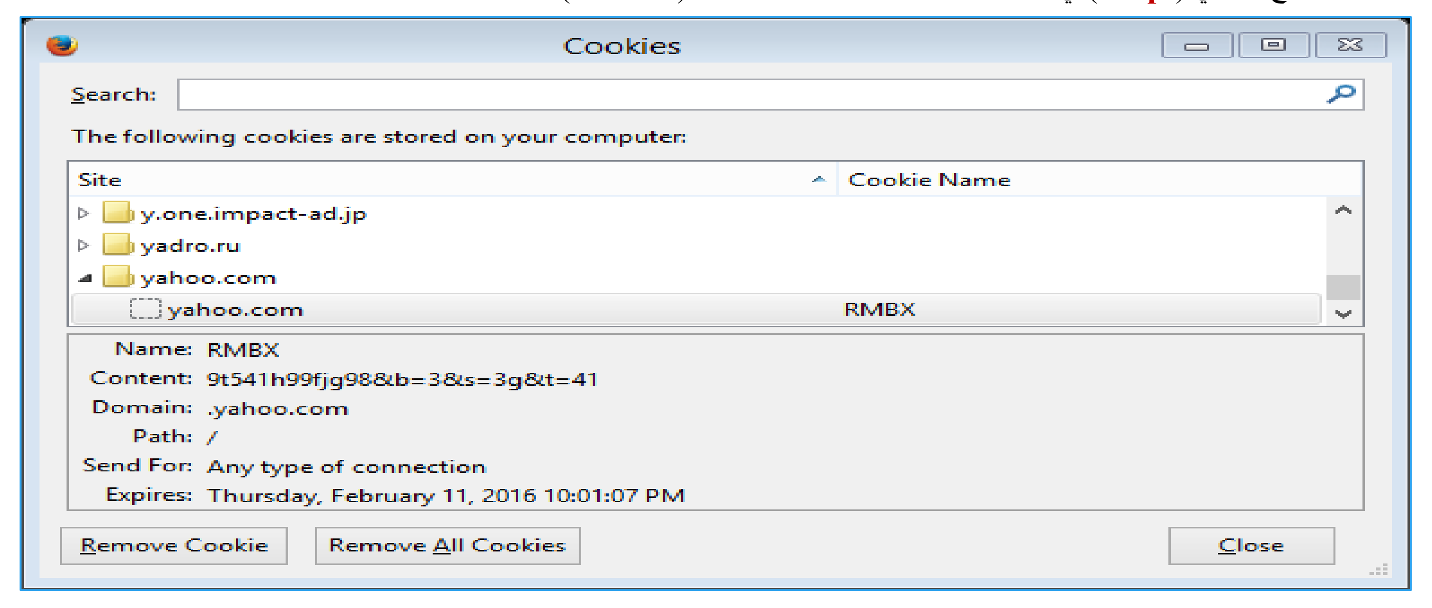
ملحوظه هذه الأداة تم تطويرها الان لتستخدم مع مستعرضي الويب الاخرين مثل جوجل كروم وغيره.

EXAMINE THE HTML SOURCE CODE (فحص اكواد صفحة HTML)

عن طريق متابعة التعليقات (**comments**) التي يتم إنشاؤها إما عن طريق نظام **CMS** أو إدراجها يدويا. قد توفر هذه التعليقات القرائن لمساعدتك على فهم ما يعمل في الخلفية. حتى هذا قد يوفر تفاصيل الاتصال الخاصة بمشرف شبكة الإنترنت (**web admin**) أو المطور (**developer**). مراقبة جميع الروابط (**links**) وعلامات الصورة (**image tags**)، من أجل تعيين بنية نظام الملفات. هذا يسمح لك بالكشف عن المجلدات والملفات المخفية. إدخال بيانات وهمية لتحديد الكيفية التي يعمل البرنامج النصي (**script**).



فحص ملفات الكوكيز (**cookies**)التي تم وضعتها بواسطة الملقم/الخادم(**server**) لتحديد البرنامج التي تم تشغيلها وسلوكها. يمكنك أيضا تحديد البرنامج النصي (**script**)في المنصات من خلال مراقبة الدورات (**sessions**) وغيرها من ملفات الكوكيز.



MIRRORING AN ENTIRE WEBSITE

مراءة المواقع (Website Mirror): هو عملية إنشاء نسخة طبق الأصل من الموقع الأصلي. ويمكن أن يتم ذلك مع مساعدة من مجموعه من الأدوات. هذه الأدوات تسمح لك بتحميل موقع على شبكة الإنترنت إلى المجلد المحلي الخاص بك، وبناء كافة المجلدات، صفحات HTML، الصور، الفلاشات، ملفات الفيديو وغيرها من الملفات من الخادم/الملقم إلى جهاز الكمبيوتر الخاص بك.

هذه العملية (Website Mirror) يحتوى على العديد من الفوائد كالاتى:

1) من المفيد تصفح المواقع في الوضع اوفلاين (**offline**).
2) يساعد في إنشاء موقع احتياطي نسخة أصلية من الموقع الأصلي.
3) يمكن عمل استنساخ للموقع ما (**website clone**).
4) مفيد في اختبار موقع ما في الوقت الذي يتم فيه تصميم وتطوير الموقع.
5) من الممكن توزيعها على خوادم/ملقمات متعددة بدلا من استخدام في ملقم واحد فقط.



FIGURE 2.17: JuggyBoy's Original and Mirrored website



Website Mirroring Tools (الأدوات المستخدمة في استنساخ المواقع)

- **HTTrack Web Site Copier**

المصدر: **http://www.httrack.com**

HTTrack هو أداة لنسخ موقع ويب من على شبكة الانترنت هذه الأداة تسهل على مختبرى الاختراق عمله حيث تعطيه الفرصة لإلقاء نظره على المحتوى الكامل لهذا الموقع وجميع صفحاته وملفاته وفى بيئة أخرى تسيطر عليها بنفسك. هذه الأداة تتيح لك تحميل موقع ويب كامل من على الإنترنت إلى مجلد محلي، وبناء كافة المجلدات، والحصول على صفحات **HTML** والصور وغيرها من الملفات من الخادم إلى جهاز الكمبيوتر الخاص بك. **HTTrack** يرتب هيكل روابط الموقع الأصلي (**Site's relative link structure**). افتح صفحة من "الموقع الذي قمنا بتحميله **website mirror** " على المتصفح الخاص بك، وتصفح الموقع من رابط إلى رابط، ويمكنك عرض الموقع كما لو كنت موجود على الإنترنت. **HTTrack** يمكنه أيضا تحديث الموقع الذى قمت بتحميله حاليا، وأيضا استئناف انقطاع التحميل.

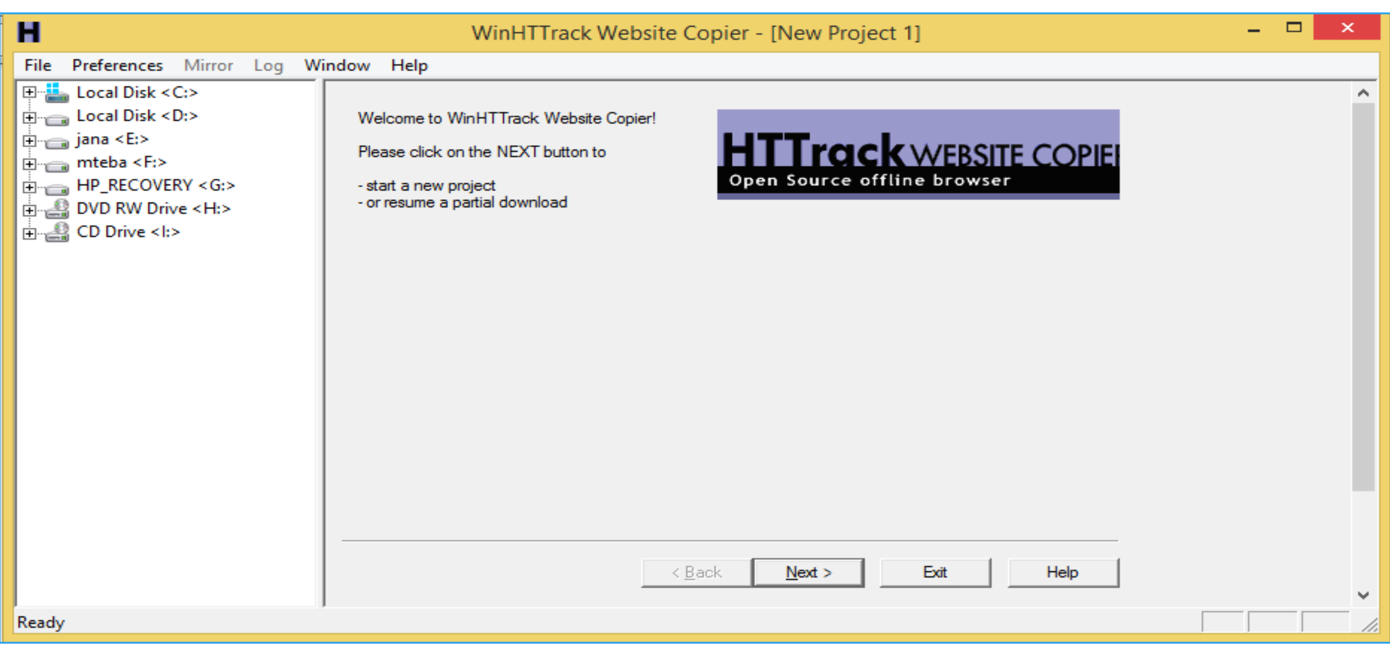
هنا سوف تتعلم نسخ موقع كامل من على شبكة الانترنت باستخدام أداة النسخ HTTrack والتي تمكنك منع هجوم D-DOS.

- **في نظام التشغيل ويندوز**

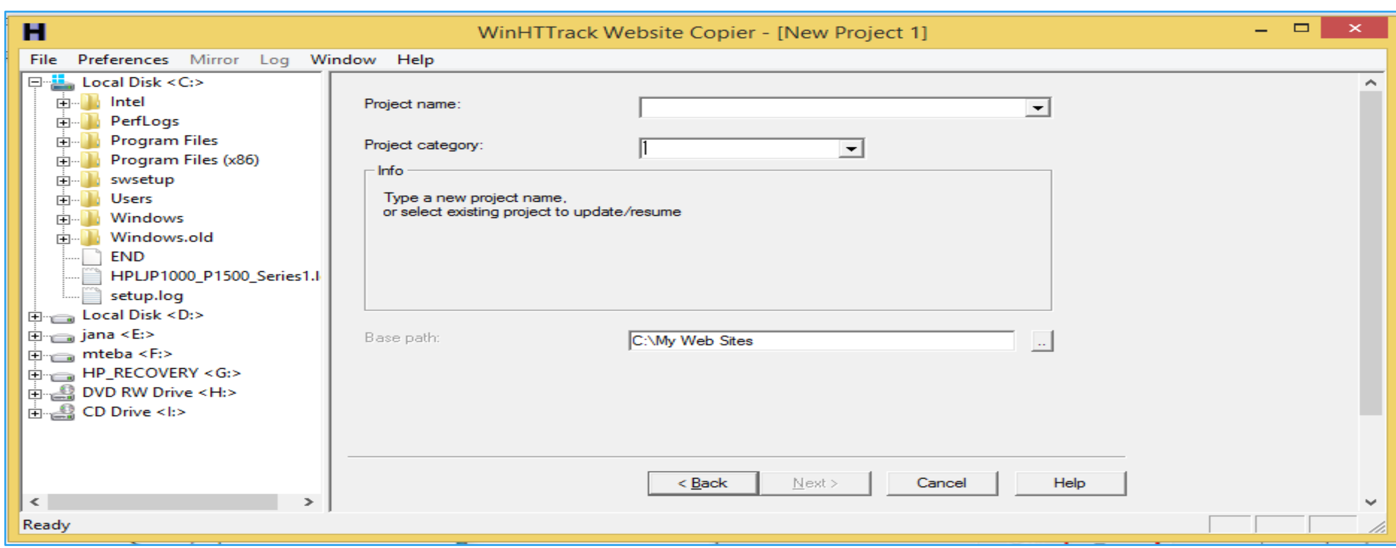
1- نعمل على تحميل هذه الأداة ثم نقوم بتثبيتها عن طريق اتباع الـ wizard الخاص به

2- نقوم بتشغيل البرنامج من خلال الأيقونة الخاصة به

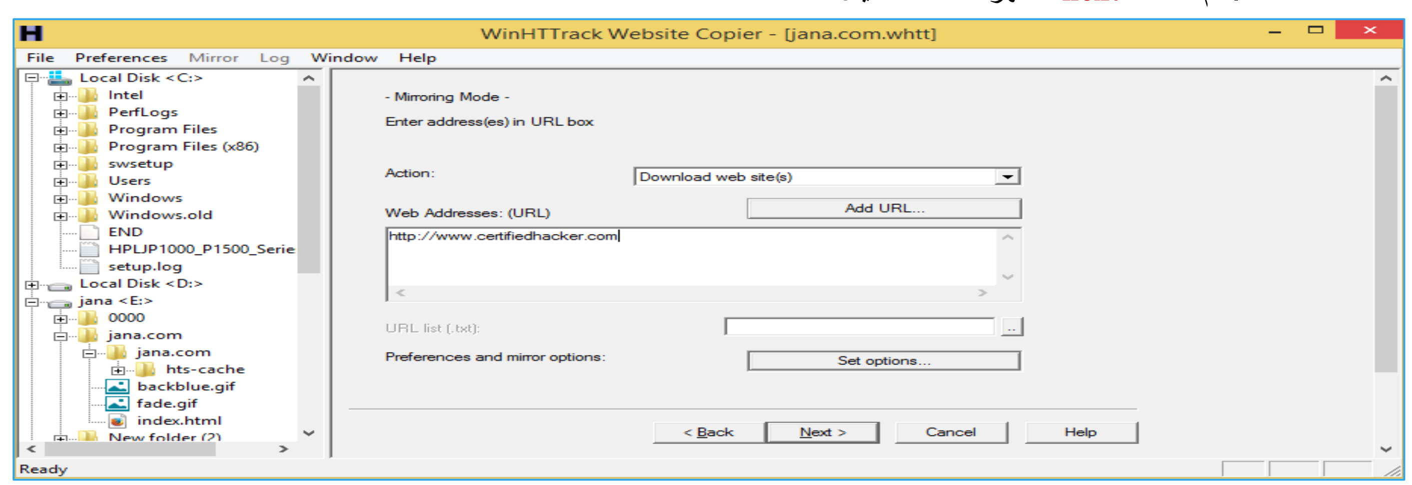
3- بعد الضغط عليه تظهر الشاشة التالية:



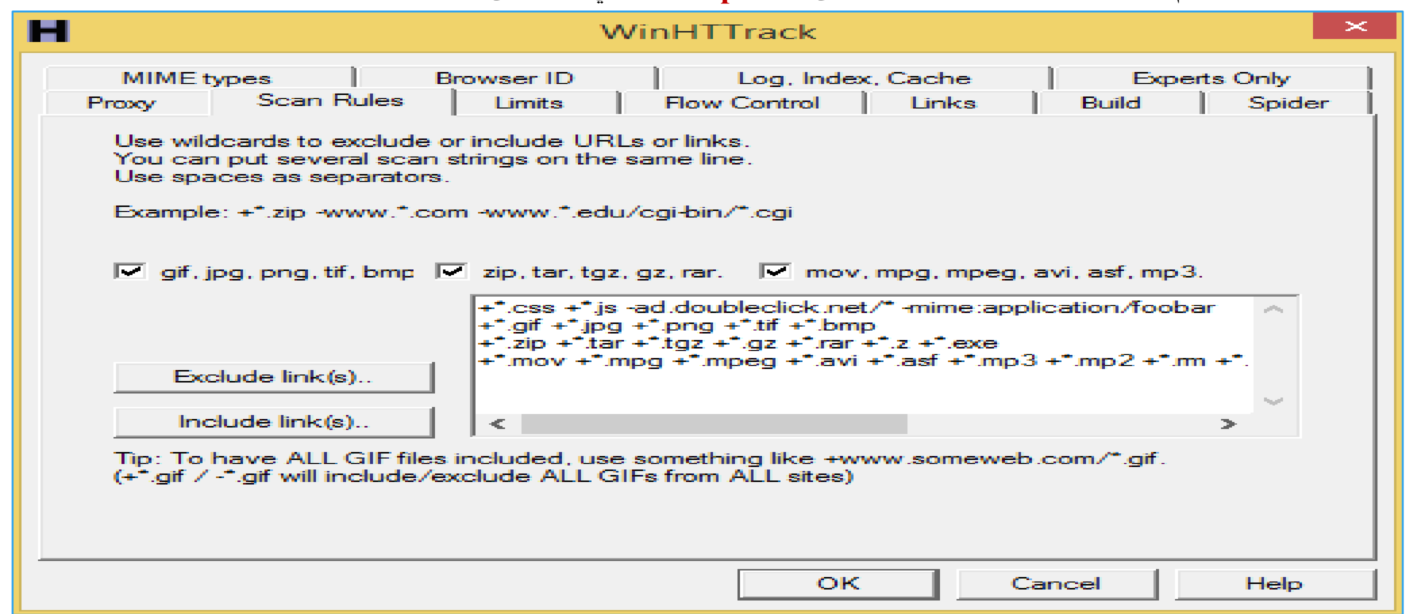
4- نقوم بالضغط على next لإنشاء مشروع جديد new project ثم نحدد اسم هذا المشروع.



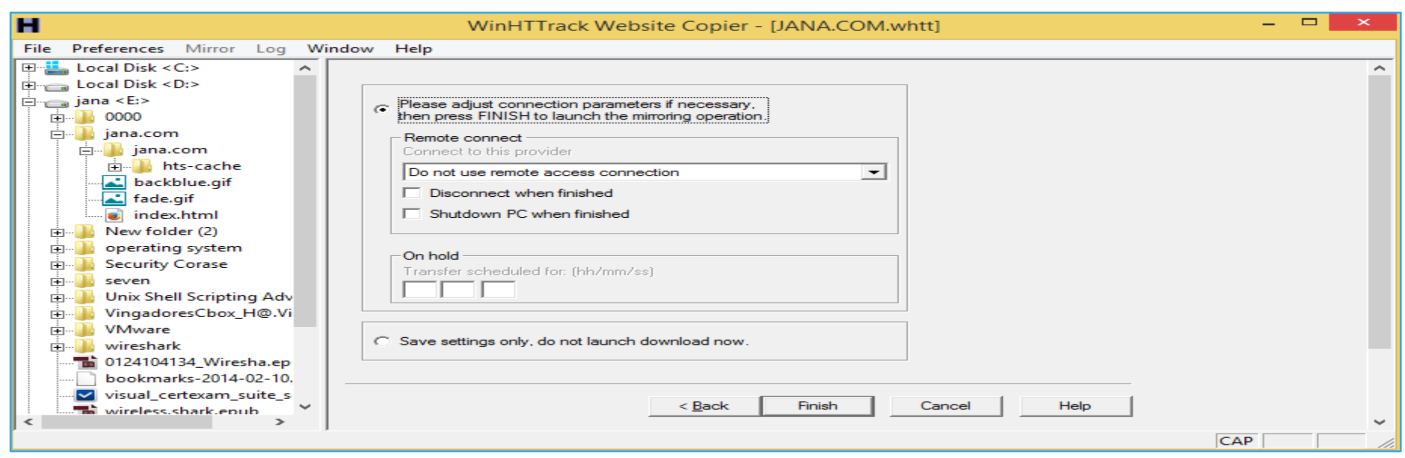
5- ندخل اسم المشروع في الخانة **Project name** وفى الخانة **Base path** نعمل على تحديد المكان الذي سوف يتم فيه تخزين الملفات. ثم نضغط **next** فتظهر الشاشة التالية:



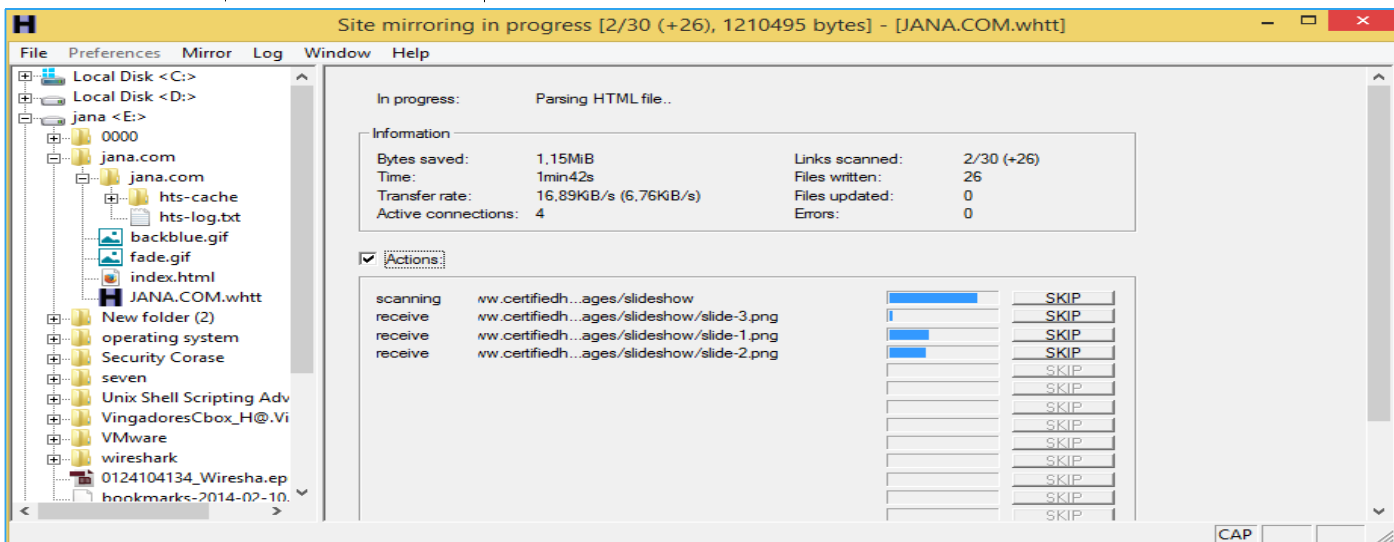
6- ندخل اسم الموقع باستخدام الزر **Add URL** ويمكن أيضا تحديد طبيعة موقع الويب المراد تحميله عن طريق **Action** ويمكن أيضا استخدام اعدادات متقدمة وذلك بالضغط على **Set options** والتي تؤدى الى ظهور الشاشة التالية:



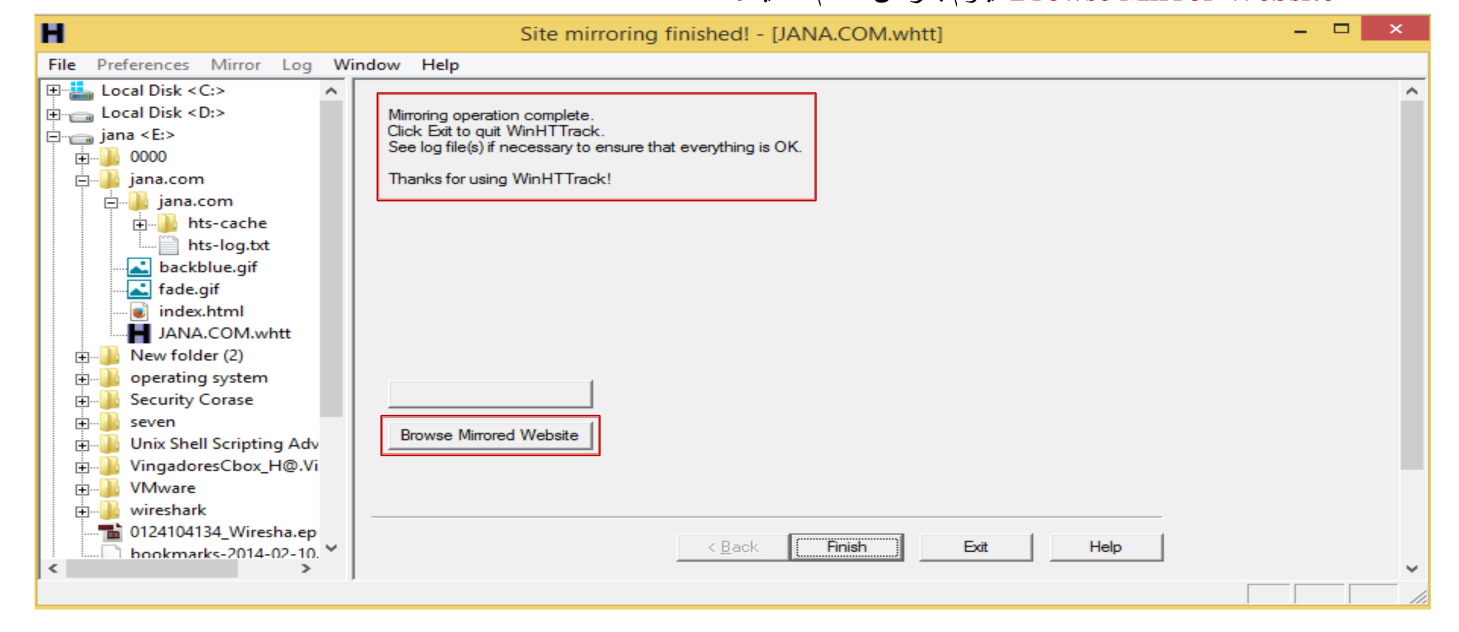
7- نجد هنا الكثير من الاعدادات المتقدمة مثل البروكسي وتحديد الحجم المسموح به للتحميل (**Limits**) وغيرها ما يهما هنا هو **Scan Rules** والتي تحدد أنواع الملفات التي نريد تحميلها وهنا نختار جميع الأنواع المتاحة ثم نضغط **ok** ثم نضغط **NEXT**.



8- عند الوصول الى هذه الشاشة نكون قد انتهينا ونترك الاعدادات الافتراضية فيها كما هيا ثم نضغط **FINISH** حتى يتم علمية التحميل.



9- بعد الانتهاء من التحميل يعطيك رسالة انه قد أنهي التحميل **Mirror Operation complete** ويوجد في اخر الشاشة زر اسمه **Browse Mirror Website** ليقوم بعرض ما تم تحميله.



- **في نظام التشغيل جنو/لينكس**

هذه الأداة مدمجة في بعض نسخ التوزيعة كالي ولكن للأسف غير مدمجة في نسخ اخرى من **كالي** وغير مدمجة في نسخة **باك تراك** لذلك سوف تحتاج الى تثبيتها في حالة عدم توفرها على النسخة الخاصة بك كالاتى:

```
root@jana:~# apt-get install httrack
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libhttrack2
Suggested packages:
  webhttrack httrack-doc
The following NEW packages will be installed:
  httrack libhttrack2
0 upgraded, 2 newly installed, 0 to remove and 574 not upgraded.
Need to get 415 kB of archives.
After this operation, 1,095 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

سوف تحتاج إلى إنشاء مجلد لتخزين ملفات موقع الويب الذي قمت بنسخه. ويتم ذلك عن طريق استخدام الامر **mkdir** وليكن اسم المجلد **mywebsites** ثم نقوم بالانتقال الى داخل المجلد كالاتى:

```
root@jana:~# mkdir mywebsites
root@jana:~# cd mywebsites/
root@jana:~/mywebsites#
```

ان عملية **HTTrack** تتم في الوضع **interactive mode** او في الوضع **non-interactive mode**. لتشغيل **HTTrack** في الوضع **interactive mode** ويتم ذلك عن طريق كتابة الامر **httrack** بدون أي صيغ والذي يؤدى الى الدخول الى الامر. ثم يبدا بسؤالك بعض الأسئلة لتحديد موقع الويب الذي تريد نسخه. اما لتشغيله في الوضع **non-interactive mode** فيتم ذلك عن طريق كتابة الامر **httrack** ثم يتبعه أي من الصيغ الاختيارية الخاصة به.

يتم تشغيل httrack في الوضع interactive mode كالاتى:

```
root@jana:~/mywebsites# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhtsjava.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :
```

نجد ان الخطوة الأولى يطلب منك اسم لهذا المشروع نقوم بإدخال اسم للمشروع **[Enter project name]** وليكن مثلا **janateba** ثم نضغط **Enter** كالاتى:

```
Enter project name :janateba

Base path (return=/root/websites/) :
```

الخطوة التالية هو اختيار المجلد الذي سوف يتم نسخ موقع الويب بداخله. قد كنا انشائنا من قبل المجلد **mywebsites** سوف نختار هذا المجلد في هذا المثال كالاتى:

```
Base path (return=/root/websites/) :/root/mywebsites

Enter URLs (separated by commas or blank spaces) :
```

الخطوة التالية يطلب منك اسم موقع الويب الذي تريد ان تقوم بنسخه وليكن مثلا www.certifiedhacker.com كالاتى:

```
Enter URLs (separated by commas or blank spaces) :www.certifiedhacker.com

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
:
```

بعد ادخال اسم الموقع يعطك خمس اقتراحات ويطلب منك ان تختار واحدا منها. يعتبر الاختيار الثاني أسهل واحد نقوم بكتابة 2 ثم الضغط على **Enter** كالاتى:

```
Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :*

You can define additional options, such as recurse level (-r<number>), separed b
y blank spaces
To see the option list, type help
Additional options (return=none) :
```

بعد ذلك يخبرك بمجموعه من الخيارات مثل نوع البروكسي الذي تريد استخدامه إذا كنت تريد استخدام بروكسي تدخل عنوانه اما إذا كنت لا تريد نقوم بالضغط على **Enter** بدون ادخال أي شيء.

بعد ذلك يريدك تحديد نوع الملفات التي تريد تحميلها هنا نكتب التعبير ***** والتي تعنى جميع أنواع الملفات ثم **Enter**. بعد ذلك إذا كنت تريد ادخال إعدادات اضافيه ام لا ثم **Enter.**

```
Additional options (return=none) :

---> Wizard command line: httrack www.certifiedhacker.com -W -O "/root/mywebsite
s/janateba"  -%v  *

Ready to launch the mirror? (Y/n) :
```

الان بعد الضغط على Enter يقوم بإخبارك بلخص بالعمليات التي سوف يقوم بها ولبد عملية النسخ نختار Y ثم Enter فيبدأ النسخ كالاتى:

```
Ready to launch the mirror? (Y/n) :Y

WARNING! You are running this program as root!
It might be a good idea to use the -%U option to change the userid:
Example: -%U smith

Mirror launched on Thu, 06 Mar 2014 19:43:06 by HTTrack Website Copier/3.46+libh
tsjava.so.2 [XR&CO'2010]
mirroring www.certifiedhacker.com * with the wizard help..
```

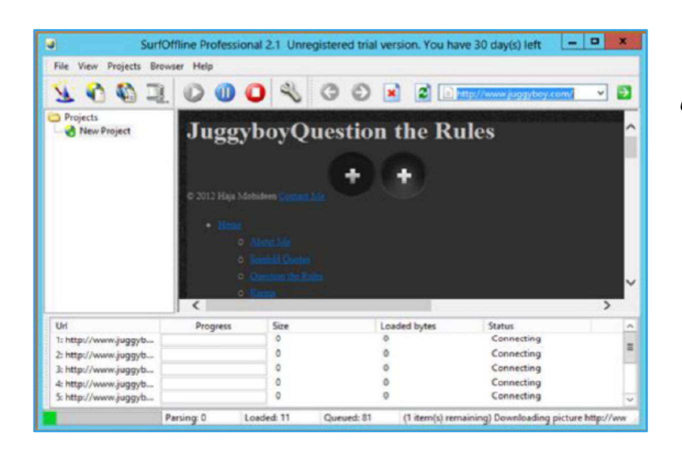
بعد الانتهاء من عملية النسخ نذهب الى المجلد الذي تم نسخ الموقع اليه ونجد انه يحتوي على ملفات الموقع كالاتى:

```
root@jana:~# ls mywebsites/janateba/
_                     hts-cache             para.llel.us
backblue.gif          hts-in_progress.lock  www.certifiedhacker.com
certifiedhacker.com   hts-log.txt           www.w3.org
fade.gif              index.html
root@jana:~#
```

- **SurfOffline**

المصدر: **http://www.surfoffline.com**

SurfOffline هو برنامج لتحميل موقع الويب. البرنامج يسمح لك بتحميل الموقع بالكامل وتحميل صفحات الويب إلى القرص الثابت الخاص بك. بعد تحميله للموقع المستهدف، يمكنك استخدام **SurfOffline** باعتباره المتصفح حاليا وعرض صفحات الويب التي تم تحميلها في ذلك. إذا كنت تفضل عرض صفحات الويب التي تم تحميلها في متصفح آخر، يمكنك استخدام معالج التصدير(**Export Wizard**) . معالج التصدير يسمح لك بنسخ المواقع بعد تحميلها إلى أجهزة الكمبيوتر الأخرى من أجل عرضها في وقت لاحق، وإعداد المواقع لحرقها لاحقا على قرص مضغوط أو قرص **DVD**.



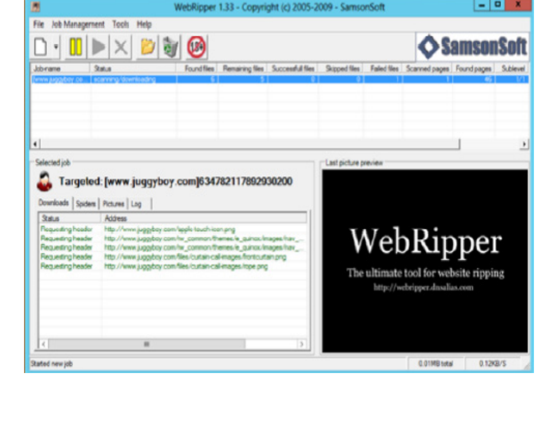
- **BlackWidow**

المصدر: **http://softbytelabs.com**

BlackWidow(الأرملة السوداء) هو ماسح ضوئي للمواقع على الإنترنت لكلا من الخبراء والمبتدئين. فإنه يفحص المواقع (انه سفاح الموقع). فإنه يمكن تحميل موقع كامل أو جزء من موقع على شبكة الإنترنت. فإنه سيقوم ببناء هيكل الموقع أولا، ثم تحميله. انه يسمح لك لاختيار ما تريد تحميله من الموقع.

- **WebRipper**

المصدر: **http://www.calluna-software.com**



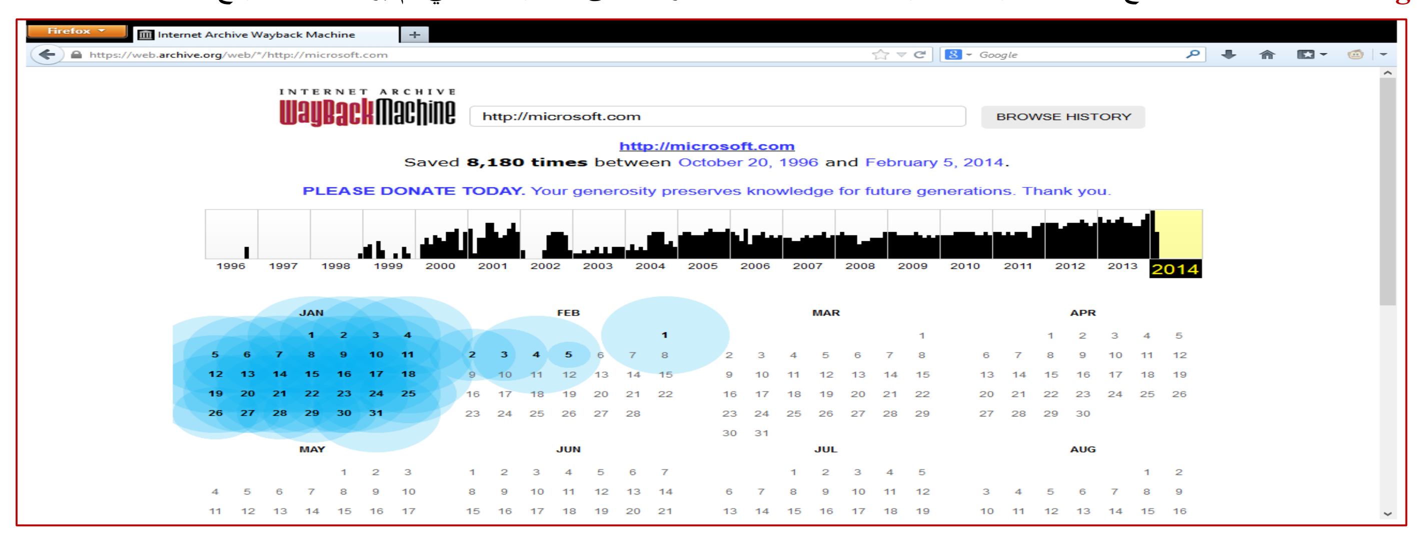
WebRipper هو ماسح محمل لمواقع الإنترنت (**Internet scanner and downloader**). اذ يعمل على تحميل كمية هائلة من الصور، والفيديو، وملفات الصوت، والوثائق القابلة للتنفيذ من أي موقع. يستخدم **WebRipper**تكنولوجيا العنكبوت(**spider-technology**) لتتبع الروابط في كل الاتجاهات بدءً بالعنوان. يتم ذلك بتصفية الملفات المثيرة للاهتمام، ويضيفها إلى قائمة انتظار التحميل، للتحميل. يمكنك تقييد العناصر التي تم تنزيلها حسب نوع الملف، والحد الأدنى لحجم الملف، والحد الأقصى لحجم الملف، وحجم الصورة. ويمكن أيضا تحميل جميع الروابط التي تكون مقيدة للكلمات الرئيسية لتجنب إضاعة **bandwidth** الخاص بك (حجم الشبكة).

<u>بالإضافة إلى الأدوات التي سبق شرحها فيما يلي بعض الأدوات الأخرى:</u>

Website Ripper Copier available at **http://www.tensons.com**
Teleport Pro available at **http://www.tenmax.com**
Portable Offline Browser available at **http://www.metaproducts.com**
Proxy Offline Browser available at **http://www.proxy-offline-browser.com**
iMiser available at **http://internetresearchtool.com**
PageNest available at **http://wwvv.pagenest.com**
Backstreet Browser available at **http://www.spadixbd.com**
Offline Explorer Enterprise available at **http://www.metaproducts.com**
GNU Wget available at **http://www.gnu.org**
Hooeey Webprint available at **http://www.hooeeywebprint.com**

استخراج معلومات عن الموقع من خلال موقع الارشيف EXTRACT WEBSITE INFORMATION FROM https://archive.org/

الأرشيف (Archive)هو عباره عن مخزن لملفات الإنترنت (**Internet Archive Wayback Machine**). يسمح لك بزيارة الإصدارات المؤرشفة عن مواقع ما. يسمح لك بجمع بعض المعلومات عن صفحات الويب الخاصة بالشركات منذ إنشائها. يقوم الموقع **www.archive.org** بتتبع صفحات الويب من وقت بدايتها، يمكنك استرداد حتى المعلومات التي تم إزالتها من الموقع الهدف.



رصد تحديثات الويب باستخدام مراقب الموقع (MONITORING WEB UPDATES USING WEBSITE WATCHER)

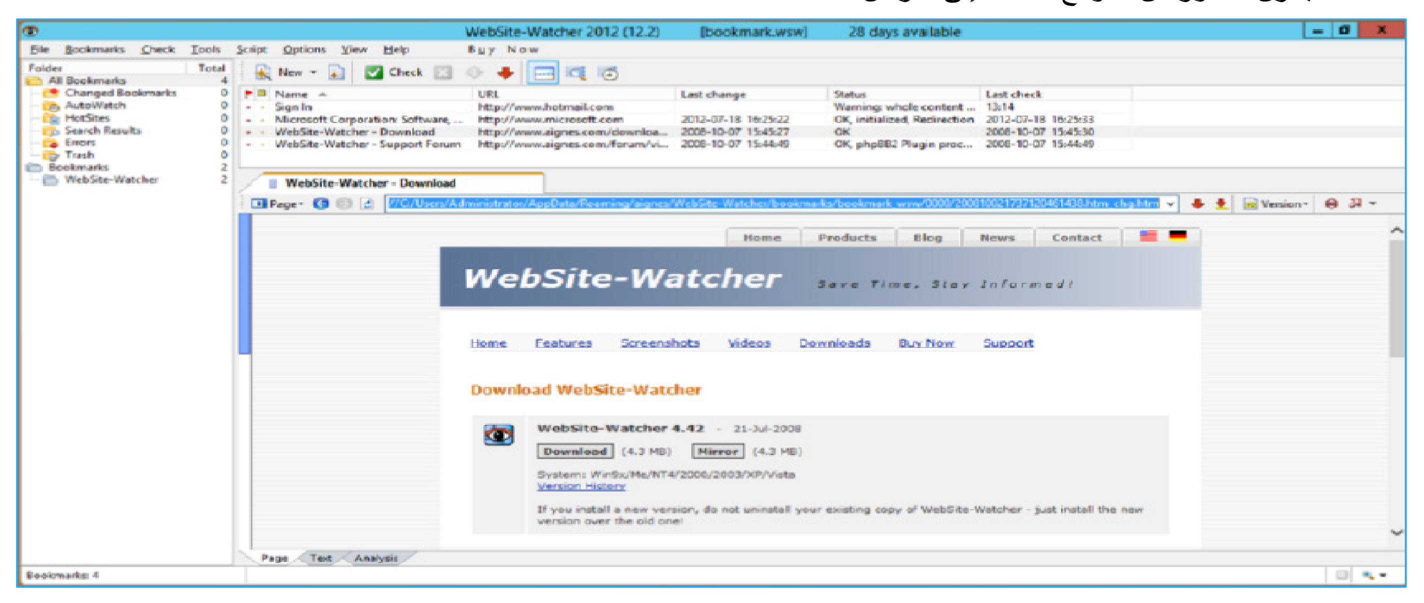
المصدر: **http://www.aignes.com**

يستخدم مراقب الموقع (**Website Watcher**) لتتبع المواقع للحصول على التحديثات والتغييرات التلقائية. عندما يحدث أي من تحديث أو تغيير، فأن مراقب الموقع تلقائيا يقوم بالكشف عنه ثم حفظ أخر إصدارين على القرص الخاص بك، ويسلط الضوء على التغيرات التي حدثت في الملف النصي. هو أداة مفيدة لرصد المواقع لاكتساب ميزة تنافسية.

الفوائد:

التحقق اليدوي المتكرر عن التحديثات ليس مطلوبا. مراقب الموقع يمكنه تلقائيا كشف وإعلام المستخدمين عن التحديثات:

- هو يتيح لك أن تعرف ما يقوم به منافسيك عن طريق فحص مواقع منافسيك.
- الموقع يمكنه تتبع إصدارات البرامج الجديدة أو تحديثات برامج التشغيل.
- يخزن الصور من المواقع المعدلة إلى القرص.



3-عمليات الاستطلاع باستخدام البريد الإلكتروني (EMAIL FOOTPRINTING)

يصف هذا القسم كيفية تعقب الاتصالات عبر البريد الإلكتروني، وكيفية جمع المعلومات من رؤوس البريد الإلكتروني، وأدوات تعقب البريد الإلكتروني.

تتبع اتصالات البريد الإلكتروني [TRACKING EMAIL COMMUNICATIONS]

تعقب البريد الإلكتروني (Email tracking) هو الأسلوب الذي يساعدك على مراقبة وكذلك تعقب رسائل البريد الإلكتروني لمستخدم معين. هذا النوع من التتبع يمكن من خلال سجلات **digitally time stamped** للكشف عن وقت وتاريخ تلقي أو فتح رسالة بريد إلكتروني بواسطة الهدف. هناك الكثير من أدوات تعقب البريد الإلكتروني متوفرة بسهولة في السوق، وذلك باستخدام ما يمكنك جمعه من المعلومات مثل الاتي: عناوين IP، خدمة البريد، ومزود الخدمة الذي تم إرسال البريد عن طريقه. المهاجمين يمكنهم استخدام هذه المعلومات لبناء استراتيجية القرصنة.

أمثلة على أدوات تعقب البريد الإلكتروني ما يلي: eMailTrackerPro و Paraben E-mail Examiner.

باستخدام أدوات تتبع البريد الإلكتروني يمكنك جمع المعلومات التالية حول الضحية:

- **الموقع الجغرافي**: تقدير وعرض موقع المتلقي على الخريطة، وربما حتى حساب المسافة من موقعك.
- **قراءة الفترة الزمنية**: مدة الوقت الذي يقضيه المتلقي على قراءة البريد المرسل من قبل المرسل.
- **كشف الوكيل proxy detection** : يوفر معلومات حول نوع الخادم المستخدم من قبل المستلم.
- **وصلات**: يسمح لك بالتحقق ما إذا كان قد تم فحص الروابط المرسلة إلى المتلقي من خلال البريد الإلكتروني أو لا.
- **نظام التشغيل**: هذا يعطيك معلومات عن نظام التشغيل المستخدم من قبل المستلم. المهاجم يمكنه استخدام المعلومات لبدء عملية الهجوم من خلال بعض الثغرات في نظام التشغيل الحالي.
- **توجيه البريد الإلكتروني (Forward Email)**: البريد الإلكتروني الذي يتم إرساله إليك يتم توجيهه إلى شخص أخر والذي يتم تحديده بسهولة عن طريق هذه الأدوات.

جمع المعلومات من خلال عناوين البريد الإلكتروني (COLLECTION FORM THE EMAIL HEADERS)

هذه الأيام أصبح البريد الإلكتروني هو أسرع وسيلة للاتصال، وتستخدم على نطاق واسع عبر البريد الإلكتروني، لأغراض شخصية ولأغراض تجارية، الآن لديك المقدرة لتحديد موقع الشخص الذي يرسل لك رسالة البريد الالكتروني ولكن كيف يمكنك أن تفعل هذا. يمكنك تتبع البريد الكتروني باستخدام رأس رسالة البريد الإلكتروني، والسؤال المطروح الآن هو ماذا يوجد في رأس البريد الإلكتروني، وكيف نستخدمه لتتبع موقع المرسل.

رأس/عناوين البريد الإلكتروني هي المعلومات التي تسافر مع كل رسالة بريد إلكتروني. هذه العناوين تحتوي على تفاصيل المرسل، معلومات التوجيه، التاريخ، الموضوع، والمستقبل. عملية عرض رأس البريد الإلكتروني يختلف مع برامج البريد المختلفة.

أكثر برامج البريد الإلكتروني استخداما:

SmarterMail Webmail – Outlook Express 4-6 – Outlook 2000-2003 – Outlook 2007 – Eudora 4.3/5.0 Entourage – Netscape Messenger 4.7 – MacMail

فيما يلي لقطة لرأس/عنزان البريد الإلكتروني والمعلومات التي تحتويها:



المهاجم يمكنه تتبع وجمع هذه المعلومات عن طريق التحليل بالتفاصيل لعناوين البريد الإلكتروني.

 أدوات تتبع البريد الإلكتروني(Email Tracking Tools)

أدوات تعقب البريد الإلكتروني تسمح لك بتعقب البريد الإلكتروني واستخراج المعلومات منه مثل هوية المرسل(**Sender identity**) ، خادم البريد(**mail server**) ، عنوان **IP** المرسل، وما إلى ذلك. يمكنك استخدام هذه المعلومات لمهاجمة أنظمة المنظمة المستهدفة عن طريق إرسال رسائل البريد الإلكتروني الخبيثة. تتوفر العديد من أدوات تعقب البريد الإلكتروني بسهوله في السوق.

وفيما يلي عدد قليل من الأدوات التي تستخدم عادة لتعقب البريد الإلكتروني:

- **eMailTrackerPro**

المصدر: http://www.emailtrackerpro.com

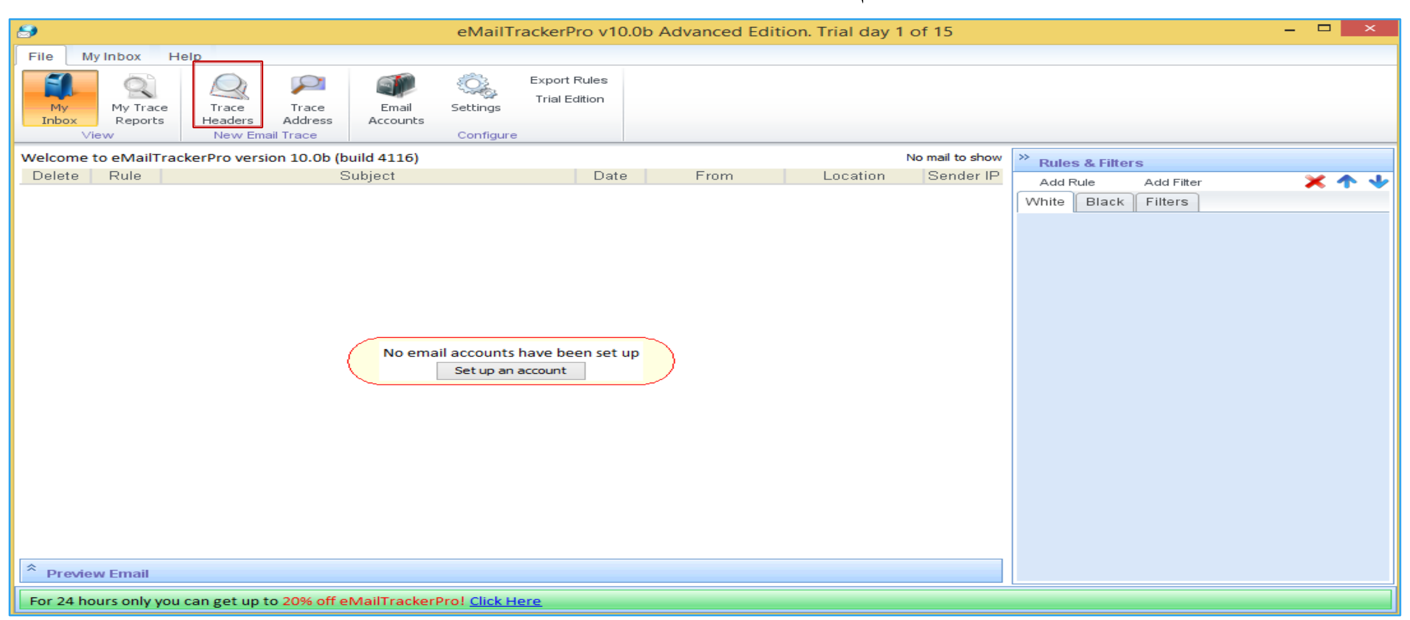
eMailTrackerPro هو أداة تعقب البريد الإلكتروني الذي يحلل رؤوس البريد الإلكتروني ويكشف عن بعض المعلومات مثل الموقع الجغرافي للمرسل وعنوان IP، وما إلى ذلك. يسمح لك أيضا باستعراض آثار في وقت لاحق عن طريق حفظ كل آثار الماضي.

تعقب البريد الإلكتروني [email tracking] هو وسيلة لرصد أو تجسس على بريد إلكتروني يتم تسليمه إلى المستلم الهدف.

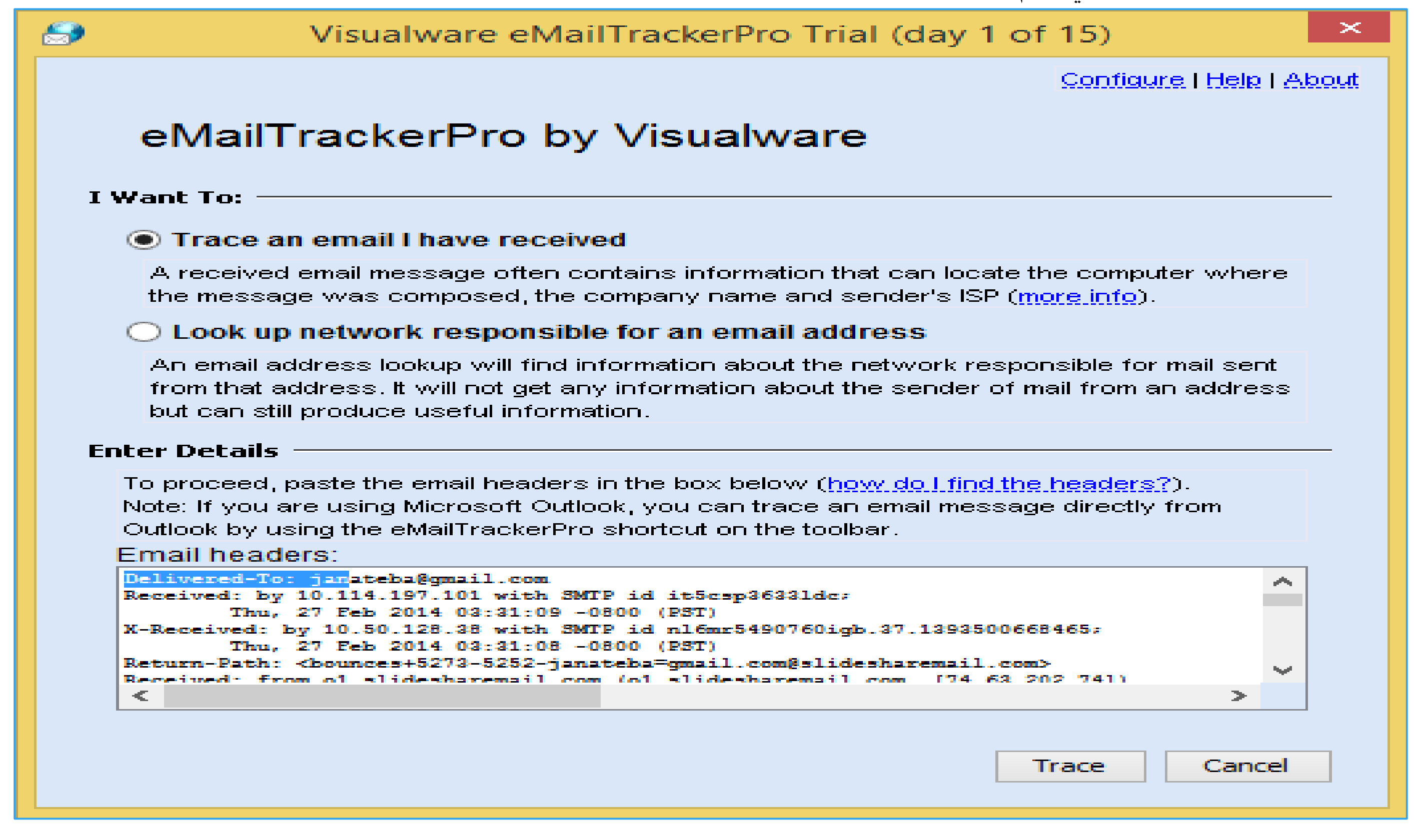
eMailTrackerPro يتيح لك تتبع البريد الإلكتروني إلى مصدره، و أيضا يستخدم لتصفية الرسائل الغير المرغوب فيها والحمولات الضارة(**SPAM EMAIL**). وعن طريق استخدام المعلومات الواردة في رأس البريد الإلكتروني(**Email header**) ، فيمكنه تحديد المدينة

أو البلدة التي نشأ منها البريد الكتروني، بما في ذلك معلومات **Whois** التي يمكنك استخدامها للإبلاغ عن سوء المعاملة وإغلاقها نهائيا.

1. يتم تثبيت هذه الأداة باتباع **wizard** الخاص بعملية التثبيت ونلاحظ أيضا انه خلال هذه العملية يتم تثبيت **java runtime** أيضا معه.
2. ملحوظه عند تثبيت البرنامج فانه يحتاج الى حساب للبريد الإلكتروني سواء من مقدمي الخدمة مثل ياهو او هوتميل او خادم خاص بك. هنا سو نتعامل مع النسخة العاشرة اما النسخة الذي تم شرحها في **CEH** هي النسخة التاسعة.
3. بعد تثبيت تطبيق **eMailTrackerPro** يتم تشغيله فتظهر الشاشة التالية:

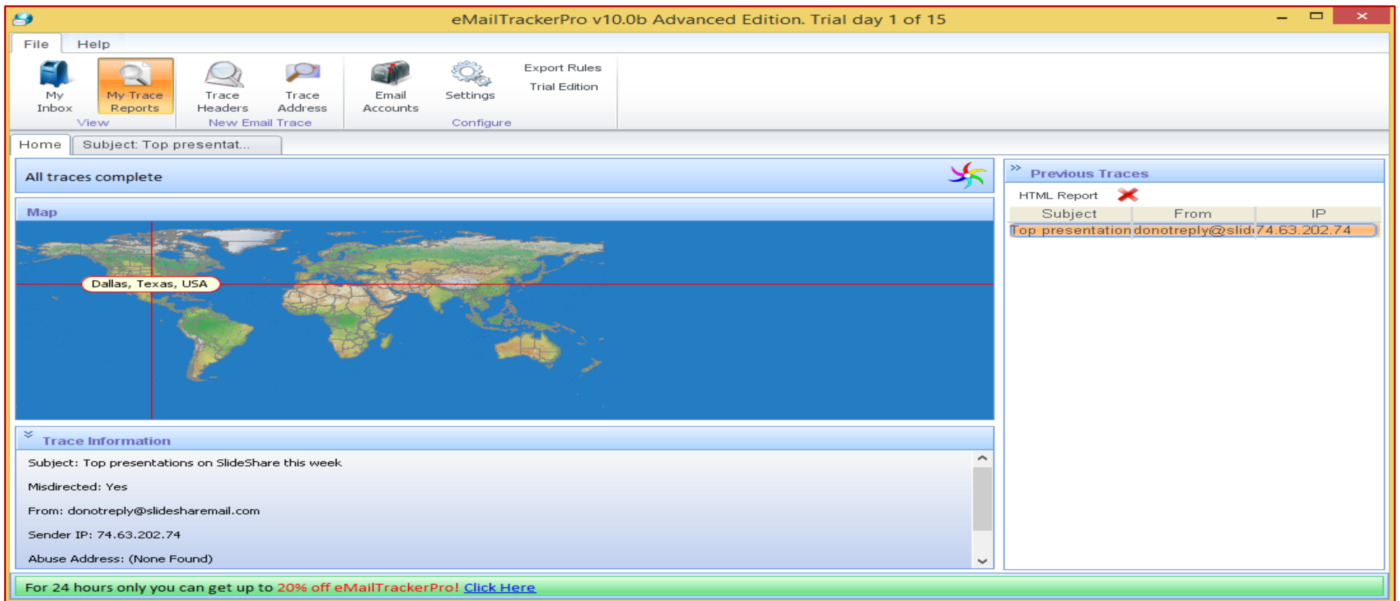


4. نلاحظ هنا انه يحتاج الى وضع بيانات الخاصة بالحساب الخاص بك في البريد الإلكتروني (**set up an account**) والتي سوف نتطرق اليه لاحقا. هنا سوف نلاحظ في شريط الأدوات وجود زر يسمى **Trace Headers** والذي يستخدم في تحليل رؤوس رسائل البريد الإلكتروني نقوم بالضغط عليه سوف يظهر لنا الشاشة التالية:



5. نختار **Trace an email I have received** ونضع راس البريد الذي استلمته في المربع الخاص **Enter Details** ثم نضغط على **Trace**.

6. بعد الضغط عليه نلاحظ انه اعطى جميع البيانات عن الذي قام بارسال هذا البريد الإلكتروني وموقعه الجغرافي وعناوين IP الخاصة به كالاتي:



- **PoliteMail**

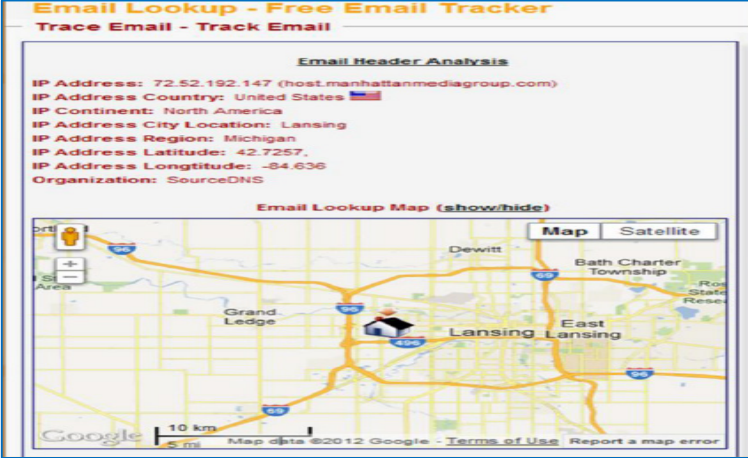
المصدر: **http://www.politemail.com**

PoliteMail هو أداة تعقب البريد الإلكتروني لبرنامج **Outlook**. وهو يتابع ويقدم تفاصيل كاملة حول من قام بفتح البريد الخاص بك واي من الوثيقة التي تم فتحها، وكذلك أي من الروابط التي تم النقر عليها وقراءتها. فإنه يوفر دمج المراسلات، اختبار الانقسام، وقائمة كاملة للإدارة بما في ذلك التجزئة. يمكنك إنشاء رسالة البريد إلكتروني تحتوي على وصلات خبيثة وإرسالها إلى موظفي المنظمة المستهدفة وتتبع هذا البريد الإلكتروني. إذا قام الموظف بالنقر على الرابط، فأنه يصبح مصابا وسيتم إعلامك بذلك. وبالتالي، يمكنك السيطرة على النظام مع مساعدة من هذه الأداة.

- **Email Lookup – Free Email Tracker**

المصدر: **http://www.ipaddresslocation.org**

Email Lookup هو أداة تعقب البريد الإلكتروني الذي يحدد عنوان **IP** الخاص بالمرسل عن طريق تحليل رأس البريد الإلكتروني. يمكنك نسخ ولصق رأس البريد الإلكتروني إلى هذه الأداة والبدء في البحث في البريد الإلكتروني عن المعلومات التي تريدها.



- **Read Notify**

المصدر: **http://www.readnotify.com**

Read Notify يوفر لك خدمة تتبع البريد الإلكتروني. وذلك بإعلامك إذا حدث فتح البريد الإلكتروني الذي تتعقبه، أو إعادة الفتح أو إعادة إرسالها. تقارير **Read Notify** لتتبع البريد الإلكتروني تتيح لك بعض المعلومات مثل تفاصيل كاملة عن مستلم الرسالة، وتاريخ ووقت فتح الرسالة والموقع الجغرافي للمتلقي، خريطة تصور الموقع، عنوان IP الخاص بالمتلقين وتفاصيل المرجع.

- **DidTheyReadIt**

المصدر: http://www.didtheyreadit.com

DidTheyReadIt هو أداة تتبع البريد الإلكتروني. من اجل استخدام هذه الأداة تحتاج إلى الاشتراك **sign up** للحصول على حساب.

ثم تحتاج إلى إضافة “DidTheyReadlt.com. " إلى نهاية عنوان البريد الإلكتروني للمستلم. على سبيل المثال، إذا كنت تريد أن ترسل رسالة بريد إلكتروني إلى **ellen@aol.com**، فإنك تكتب العنوان كالاتى (**ellen@aol.com.DidTheyReadlt.com**)، ومستقبل هذه الرسالة ellen@aol.com لن يرى ما قمت بإضافته (**DidTheyReadlt.com.**) إلى عنوان البريد الإلكتروني. هذه الأداة تعمل على تتبع كل البريد الإلكتروني التي ترسلها بالخفاء، دون تنبيه المتلقي. إذا يفتح المستخدم البريد الخاص بك، فإنه يخبرك عن طريق البريد الإلكتروني الخاص بك انه تم فتح الرسالة، وكم من الوقت استغرق والرسالة مفتوحة، ثم يحدد لك الموقع الجغرافي للمكان الذي حدث فتح للرسالة فيه.

- **TraceEmail**

المصدر: **http://whatismyipaddress.com**

تحاول الأداة **TraceEmail** لتحديد عنوان IP المصدر من البريد الإلكتروني استنادا إلى رؤوس البريد الإلكتروني. تحتاج فقط إلى نسخ ولصق الرؤوس بالكامل من البريد الإلكتروني المستهدف في مربع الرؤوس ثم انقر فوق (**Get Source**) للحصول عليه بيان تحليل رأس البريد الإلكتروني والنتائج. لا تملك أداة تحليل رأس البريد الإلكتروني القدرة على الكشف عن رسائل البريد الإلكتروني ذات الرؤوس المزورة. هذه الرؤوس المزورة للبريد الإلكتروني شائعة في البريد الإلكتروني الخبيث والبريد المزعج. هذه الأداة تفترض أن جميع خوادم/ملقمات البريد وعملاء البريد الإلكتروني في مسار الانتقال جديرة بالثقة.

- **MSGTAG**

المصدر: **http://www.msgtag.com**

MSGTAG هو أداة ذات بيئة ويندوز تعمل على تتبع البريد الإلكتروني والتي تستخدم تكنولوجيا (**read receipt**) والتي تخبرك عندما يتم فتح رسائل البريد الإلكتروني الخاصة بك وخاصة عندما يتم قراءة رسائل البريد الإلكتروني الخاصة بك فعلا. هذا البرنامج يضيف المسار والتتبع التي هي فريدة من نوعها إلى كل البريد الإلكتروني التي تحتاج إليها لتأكيد التسليم. عند فتح البريد الإلكتروني يتم إرسال رمز تعقب البريد الإلكتروني إلى نظام تتبع البريد الإلكتروني**MSGTAG** ويتم تسليم رسالة بريد إلكتروني إليك تخبرك بذلك. **MSGTAG** سوف يخبرك عندما يتم قراءة الرسالة عبر التأكيد عبر البريد الإلكتروني، رسالة منبثقة، أو رسالة نصية قصيرة**SMS** .

- **Zendio**

المصدر: **http://www.zendio.com**

Zendio، هو تطبيق تعقب البريد الإلكتروني وهو عباره عن إضافة لل Outlook، يقوم بإعلامك بمجرد أن يقوم المتلقي بقرائه البريد الإلكتروني، حتى تتمكن من متابعته، بمجرد قراءة الرسالة فانك تعرف بذلك وإذا قام بالنقر على أي من الروابط أيضا المدرجة في البريد الإلكتروني.

- **Pointofmail**

المصدر: **http://www.pointofmail.com**

Pointofmail.com هو دليل لخدمة استلام وقراءة البريد الإلكتروني. فإنه يضمن قراءة المستلم للرسالة، ويتتبع الملحقات، ويتيح لك تعديل أو حذف الرسائل المرسلة. فإنه يوفر معلومات مفصلة عن المتلقي، والتاريخ الكامل عن البريد الإلكتروني الذي قام بالقراءة والتوجيه، والروابط ومرفقات التتبع، والبريد الإلكتروني، والويب والرسائل SMS الإخطارات.

- **Super Email Marketing Software**

المصدر: http://www.bulk-email-marketing-software.net

هو برنامج ذات مستوى احترافي ومستقل لمجموعه من برامج الإميل (البريد الإلكتروني). فهو لديه القدرة على إرسال رسائل إلى قائمة عناوين. وهو يدعم كل من النص وكذلك رسائل البريد الإلكتروني بتنسيق **HTML**. تتم إزالة كافة عناوين البريد الإلكتروني المكررة تلقائيا باستخدام هذا التطبيق. يتم إرسال كل رسالة بريد إلكتروني بشكل فردي إلى المتلقي لذلك فإن المتلقي يرى البريد الإلكتروني فقط في رأس البريد الإلكتروني. يحفظ عناوين البريد الإلكتروني للرسائل المرسلة بنجاح فضلا عن الرسائل التي فشلت في الإرسال إلى ملف نص، **CSV**، **TSV** أو ملف **Microsoft Excel**.

- **WhoReadMe**

المصدر: http://whoreadme.com

WhoReadMeهو أداة تتبع البريد الإلكتروني. ويكون غير مرئي تماما بالنسبة للمتلقي. المتلقون لن يكون لديهم أي فكرة أن رسائل البريد الإلكتروني المرسلة إليهم يجري تعقبها. يتم إخطار المرسل في كل مرة يقوم المستلم بفتح البريد المرسل من قبل المرسل. انه يقوم بتتبع المعلومات مثل نوع نظام التشغيل والمتصفح الذي تستخدمه، **Active X controls**، نسخة**CSS** ، والمدة بين إرسال الرسائل وقراءتها، الخ.

- **GetNotify**

المصدر: **http://www.getnotify.com**

GetNotify أداة تعقب البريد الإلكتروني التي ترسل إخطارا عندما يقوم المتلقي بفتح وقرأه البريد. يرسل الإخطارات دون علم المستلم.

- **G-Lock Analytics**

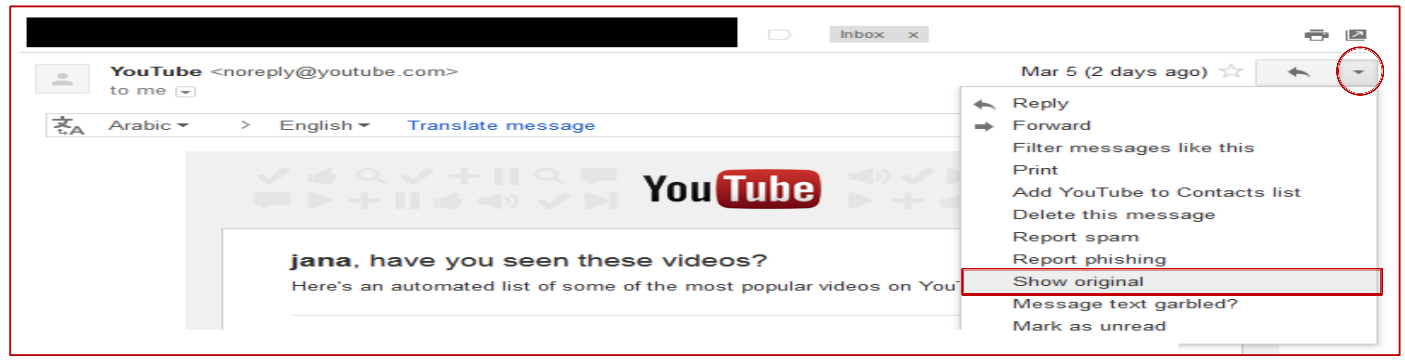
المصدر: **http://glockanalytics.com**

G-Lock Analytics هي خدمة تتبع البريد الإلكتروني. هذا يسمح لك أن تعرف ما يحدث لرسائل البريد الإلكتروني بعد إرسالها. تقارير هذه الأداة بالنسبة لك هو كم مرة تم طباعة البريد الإلكتروني وإرسالها.

كيفية الحصول على بيانات رؤوس البريد الإلكتروني:

- **In Gmail**

ندخل على الحساب الخاص بنا، ثم نذهب الى Inbox، ثم نضغط على الرسالة التي نريد تعقبها. فينتقل الى شاشة أخرى تحتوي على مضمون الرسالة. بعد الدخول الى الرسالة نضغط على الاتي ونختار **Show Original** كالاتي:

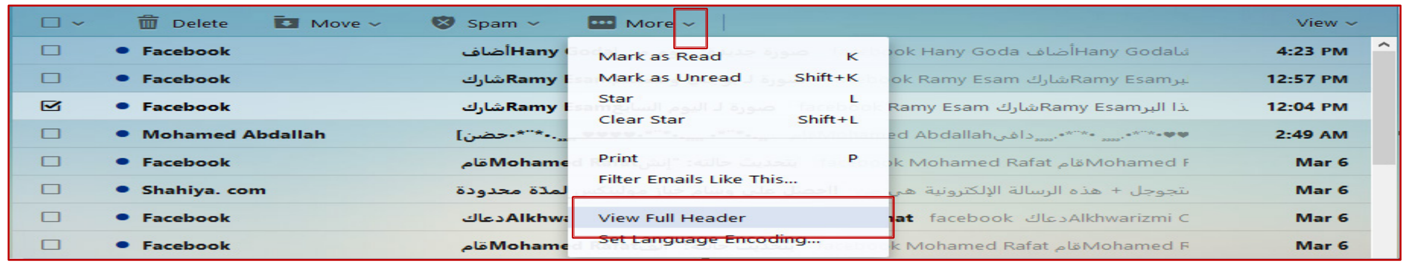


- **In Hotmail**

نفعل مثل ما حدث مع **Gmail** ولكن بدلا من الدخول على مضمون الرسالة نقوم بالضغط بالزر الايمن للماوس على الرسالة فتظهر قائمة نختار منها **view message source**.

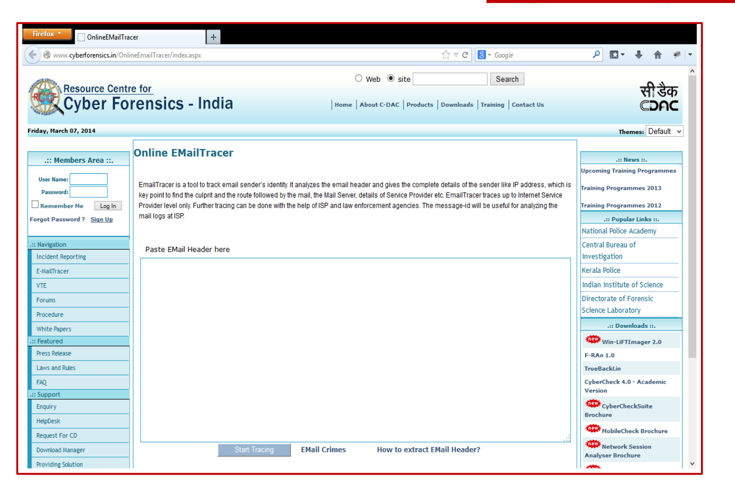
- **In yahoo**

ندخل على الحساب الخاص بنا، ثم نذهب الى**Inbox** ، ثم نضغط على الرسالة التي نريد تعقبها.ثم نذهب الى القائمة العلوية توجد علامة بجانب **More** نضغط عليها فتظهر قائمة نختار منها **view Full Header** كالاتي:



- **Online Email Tracer**

المصدر: **http://www.cyberforensics.in/OnlineEmailTracer/index.aspx**



Email Tracer هو أداة لتعقب البريد الإلكتروني لهوية المرسل. يحلل رأس البريد الإلكتروني ويعطي تفاصيل كاملة عن المرسل مثل عنوان IP، والتي هي النقطة الأساسية للعثور على المرسل والمسار الذي اتبعته البريد، خادم البريد، وتفاصيل مقدم الخدمة الخ **Email Tracer** يتتبع البريد الإلكتروني الى ما يصل إلى مستوى موفر خدمة إنترنت.

يمكن لخوادم/ملقمات (server) البريد الإلكتروني ان توفر ثروة من المعلومات للمتسللين ومختبري الاختراق. في نواح كثيرة، البريد الإلكتروني يشبه الباب الدوار للمنظمة المستهدفه الخاصة بك. على افتراض ان الهدف يملك ملقم/خادم للبريد الإلكتروني الخاصة به، هذا هو في كثير من الأحيان مكانا رائعا للهجوم. من المهم أن نتذكر، " لا يمكنك منع ما يجب أن تسمح به" بعبارة أخرى، لإعداد البريد الإلكتروني بشكل صحيح، فان حركة المرور الخارجية (external traffic) يجب أن تمر من الأجهزة الخاصة بك مثل جدران الحماية والموجهات (routers)، إلى الجهاز الداخلي، وعادة ما يكون داخل الشبكات المحمية الخاصة بك. نتيجة لهذا، نحن غالبا ما يمكن جمع قطع كبيرة من المعلومات من خلال التفاعل المباشر مع ملقم/خادم البريد الإلكتروني. واحد من أول الأشياء التي يجب القيام به عند محاولة خداع خادم البريد الإلكتروني هو إرسال رسالة بريد الإلكتروني تحتوي على ملف فارغ غير ضار سواء (.bat) او (.exe) مثل (calc.exe). إن الهدف من هذه الحالة هو إرسال رسالة إلى خادم البريد الإلكتروني المستهدف الموجود داخل المنظمة الهدف على أمل انها تملك خادم البريد الإلكتروني، ومن ثم يتم رفض الرسالة.

بمجرد رفض الرسالة يتم إرجاعها إليك، وهنا يمكننا محاولة انتزاع معلومات حول ملقم البريد الإلكتروني الهدف. في كثير من الحالات، يكون نص الرسالة التي تم رفضها وارجاعها اليك هو أن الملقم لا يقبل رسائل البريد الإلكتروني مع ملحقات يحتمل أن تكون خطيرة. غالبا ما تشير هذه الرسالة بمورد محدد ونسخة مضاد الفيروسات التي تم استخدامها لفحص البريد الإلكتروني. هذه قطعة كبيرة من المعلومات. وجود رسالة الرد من خادم البريد الإلكتروني المستهدفة يسمح لنا أيضا بتفقد رؤوس البريد الإلكتروني. والتي تسمح لنا لاستخراج بعض المعلومات الأساسية حول خدمة البريد الإلكتروني، بما في ذلك عناوين IP وإصدارات برامج معينة أو العلامة التجارية من خادم البريد الإلكتروني. معرفة عنوان IP واصدارات البرمجيات تكون مفيدة بشكل لا يصدق عندما ننتقل إلى مرحلة exploitation phase.

4-COMPETITIVE INTELLIGENCE (الاستخبارات التنافسية)

الاستخبارات التنافسية هي عملية تجميع وتحليل، وتوزيع المعلومات الاستخبارية حول المنتجات والعملاء والمنافسين، والتكنولوجيات باستخدام الإنترنت. هذه المعلومات التي يتم جمعها يمكن أن تساعد المديرين والمسؤولين التنفيذيين في شركة ما من اتخاذ قرارات استراتيجية. هذا القسم هو عباره عن جمع المعلومات الاستخبارية التنافسية والمصادر حيث يمكنك الحصول على معلومات قيمة.

COMPETITIVE INTELLIGENCE GATHERING (جمع المعلومات الاستخباراتية)

يوجد العديد من الأدوات المختلفة المتوفرة في السوق لغرض جمع المعلومات الاستخبارية التنافسية.
يعرف هذا بالحصول على معلومات حول المنتجات، المنافسين، وتقنيات الشركة باستخدام الإنترنت كوسيلة الاستخبارات التنافسية.
الاستخبارات التنافسية ليس فقط عن تحليل المنافسين ولكن أيضا عن تحليل منتجاتها والعملاء والموردين، الخ التي تؤثر على المنظمة. هذه العملية تكون دقيقه ومن غير تدخل في طبيعتها مقارنة بسرقة الملكية الفكرية مباشرة والتي نفذت من خلال القرصنة أو التجسس الصناعي.
هذه العملية تركز بشكل رئيسي على بيئة الأعمال الخارجية. إنها تعمل على تجميع المعلومات بطريقه أخلاقية وقانونيه بدلا من جمعها سرا. وفقا لـ CI professionals، بأنه إذا كانت المعلومات الاستخباراتية التي جمعت ليست مفيدة، فإنه لا يسمى Intelligence. يتم تنفيذ الاستخبارات التنافسية لتحديد:

- ما يفعله المنافسين.
- كيف يقوم المنافسين بوضع منتجاتهم وخدماتهم.

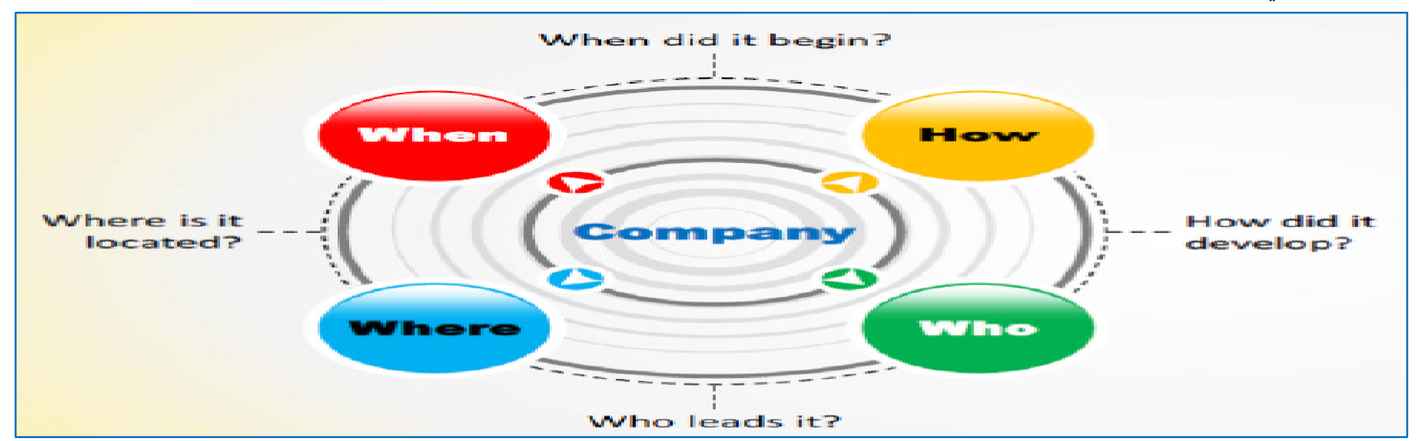
<u>مصادر الاستخبارات التنافسية:</u>

- المواقع الإلكترونية للشركة وإعلانات التوظيف.
- محركات البحث، الإنترنت، وقواعد البيانات على الإنترنت.
- البيانات الصحفية والتقارير السنوية.
- المجلات التجارية، المؤتمرات، والصحف.
- براءات الاختراع والعلامات التجارية.
- الهندسة الاجتماعية.
- كتالوجات المنتجات ومنافذ البيع بالتجزئة.
- المحلل والتقارير التنظيمية.
- مقابلات العملاء والموردين.
- الوكلاء والموزعين والموردين.

يمكن أن تتم عملية الاستخبارات التنافسية إما عن طريق توظيف الناس للبحث عن المعلومات أو من خلال الاستفادة من خدمة قاعدة البيانات التجارية، والتي تتكبد أقل تكلفة من توظيف أفراد لتفعل الشيء نفسه.

الاستخبارات التنافسية –متى بدأت هذه الشركة[WHEN DID THIS COMPANY BEGIN] ؟ وكيف تطورت؟

جمع الوثائق والسجلات الخاصة بالمنافسين التي تم جمعها تساعد على تحسين الإنتاجية والربحية وتحفيز النمو. فإنه يساعد على تحديد إجابات لما يلي:



- **متى بدأت الشركة (When did it begin)؟**

من خلال الاستخبارات التنافسية، وتاريخ الشركة التي يمكن جمعها، مثل متى تأسست شركة معينة. في بعض الأحيان، المعلومات الهامة الغير متوفرة عادة للآخرين يمكن أيضا جمعها.

- **كيف تطورت الشركة (How did it develop)؟**

من المفيد جدا المعرفة حول كيفية تطور شركة معينة. ما هي الاستراتيجيات المختلفة التي تم استخدامها من قبل هذه الشركة؟ سياسة الإعلان عنها، إدارة العلاقات العامة، وغيرها من الاستراتيجيات التي يمكن تعلمها.

- **من الذي يقود هذا (Who leads it)؟**

تساعد هذه المعلومات شركة ما في تعلم التفاصيل عن الشخص الرائدة (صانع القرار) في الشركة المنافسة.

- **أين تقع الشركة (Where is it located)؟**

موقع الشركة والمعلومات ذات الصلة لمختلف فروعها وعملياتها يمكن جمعها من خلال الاستخبارات التنافسية. يمكنك استخدام هذه المعلومات التي تم جمعها من خلال الاستخبارات التنافسية لبناء استراتيجية القرصنة.

فيما يلي بعض من المواقع التي تكون مصدرا للمعلومات التي تساعد المستخدمين الحصول على معلومات استخباراتية تنافسية.

- **EDGAR**

المصدر: http://www.sec.gov/edgar.shtml

جميع الشركات، الأجنبية والمحلية، تحتاج إلى تقديم بيانات التسجيل، التقارير الدورية، وأشكال أخرى إلكترونيا من خلال **EDGAR**. بحيث يمكن لأي شخص رؤية قاعدة بيانات **EDGAR** بحرية من خلال شبكة الإنترنت (الويب أو FTP). جميع الوثائق التي قدمت إلى اللجنة من قبل الشركات العامة قد لا تكون متاحة على **EDGAR**.

- **Hoovers**

المصدر: http://www.hoovers.com

Hoovers هي شركة للبحوث التجارية التي توفر تفاصيل كاملة عن الشركات والصناعات في جميع أنحاء العالم. يوفر **Hoovers** المعلومات المتصلة بالأعمال التجارية من خلال الإنترنت، البيانات(**data feeds**) ، الأجهزة اللاسلكية(**wireless**)، الاتفاقات العلامة التجارية المشتركة مع الخدمات الأخرى عبر الإنترنت. أنه يعطي معلومات كاملة عن المنظمات، والصناعات، والناس التي تدفع الاقتصاد. توفير الأدوات لربط الأشخاص المناسبين أيضا، من أجل الحصول على العمل المنجز.

- **LexisNexis**

المصدر: http://lexisnexis.com

LexisNexis هو المزود العالمي لتمكين المحتوى وحلول مصممة خصيصا للمهنيين العاملين في القانون، إدارة المخاطر، الشركات، الحكومة، منفذي القانون، المحاسبة، والأسواق الأكاديمية. فإنه يحافظ على قاعدة بيانات الإلكترونية من خلالها يمكنك الحصول على السجلات العامة القانونية والمعلومات ذات الصلة. الوثائق والسجلات، والأخبار، ومصادر الأعمال تكون في متناول العملاء.

- **Business Wire**

المصدر: **http://www.businesswire.com**

Business Wire هي الشركة التي تركز على توزيع النشرات الصحفية والإفصاح التنظيمي. توزع النشرات الإخبارية كاملة النص، والصور، ومحتوى الوسائط المتعددة الأخرى عن آلاف الشركات والمنظمات من قبل هذه الشركة في جميع أنحاء العالم على الصحفيين ووسائل الإعلام، والأسواق المالية، والمستثمرين، والمعلومات على شبكة الإنترنت، وقواعد البيانات، والجمهور العام. هذه الشركة لديها شبكتها الإلكترونية الخاصة والتي من خلالها يتم تصدير النشرات الإخبارية.

الاستخبارات التنافسية -ما هي خطط الشركة(WHAT ARE THE COMPANY'S PLANS) ؟

فيما يلي بعض الأمثلة لمواقع الويب المفيدة في جمع المعلومات المهمة عن العيد من الشركات وخططهم:

MarketWatch
THE WALL STREET JOURNAL.

المصدر: **http://www.marketwatch.com**

MarketWatch يقيس نبض الأسواق. يوفر الموقع أخبار الأعمال، المعلومات الشخصية والمالية، الأدوات والبيانات الاستثمارية، مع العديد من الصحفيين المخصصين يمكنهم توليد المئات من العناوين والقصص، أشرطة الفيديو، وموجزات السوق يوميا.

twst.com

المصدر: **http://www.twst.com**

Wall Street Transcript هو موقع ويب ينشر تقارير الصناعة يحتاج إلى دفع الاشتراك للنشر. أنه يعبر عن وجهات نظر مديري المال ومحللي الأسهم في قطاعات الصناعة المختلفة. وتنشر مقابلات مع كبار المديرين التنفيذيين من الشركات.

LIPPER MARKETPLACE

المصدر:**http://www.lippermarketplace.com**

LipperMarketplace تقدم حلولا على شبكة الإنترنت التي هي مفيدة لتحديد القيمة السوقية للشركة. السوق يساعد في تأهيل وتوفير الاستخبارات التنافسية اللازمة لتحويل هذه الآفاق إلى العملاء. حلولها تسمح للمستخدمين لتحديد صافي التدفقات وتتبع الاتجاهات المؤسسية.



المصدر: **http://www.euromonitor.com**

يوفر **Enuromonitor** البحوث الاستراتيجية بالنسبة للأسواق الاستهلاكية. وهي تنشر تقارير عن الصناعات والمستهلكين، والعوامل الديموغرافية. أنه يوفر أبحاث السوق والدراسات الاستقصائية التي تركز على احتياجات مؤسستك.

Fagan Finder

المصدر: **http://www.faganfinder.com**

FaganFinder هو عبارة عن مجموعة من أدوات الإنترنت. بل هو دليل لمواقع المدونات (**blog sites**)، ومواقع الأخبار، ومحركات البحث، ومواقع مشاركة الصور، ومواقع العلوم والتعليم، الخ. يحتوي على أدوات متخصصة مثل الترجمة ومعالج المعلومات **URL** والتي تتوفر للعثور على معلومات حول مختلف الإجراءات مع صفحة الويب.

SEC Info

المصدر: **http://www.secinfo.com**

SEC Info يقدم خدمة قاعدة البيانات عن المعلومات عن الأوراق المالية والبورصات الأمريكية (**SEC**) على شبكة الإنترنت، مع المليارات من الروابط التي تضاف إلى وثائق **SEC**. لأنها تتيح لك البحث عن طريق الاسم، الصناعة، والأعمال التجارية، و**SIC**، رمز رمز المنطقة، رقم الملف، CIK، المواضيع، الرمز البريدي، الخ.

THE SEARCH MONITOR
PAID • ORGANIC • LOCAL • SHOPPING • SOCIAL

المصدر: **http://www.thesearchmonitor.com**

يوفر **The Search Monitor** الاستخبارات التنافسية في الوقت الحالي لمراقبة عدد من الأمور. فإنه يسمح لك بمراقبة الحصه السوقية، رتبة الصفحة، نسخة الإعلانية، صفحات الهبوط، وميزانية منافسيك. مع رصد العلامات التجارية، يمكنك مراقبة شركتك وكذلك العلامة التجارية لمنافسك ومع جهاز العرض التابعة لها، يمكنك مشاهدة الشاشة الإعلانية ونسخه من الصفحة المقصودة.



- **Copernic Tracker**

المصدر: http://www.copernic.com

Copernic هو تطبيق لتتبع البرمجيات. تعمل على مراقبة مواقع الويب الخاصة بالمنافسين بشكل مستمر ويبلغك بأي تغييرات في المحتوى عبر البريد الإلكتروني، إن وجدت. يسلط الضوء على الصفحات التي تم تحديثها فضلا عن التغييرات التي أدخلت على الموقع حسب ما تريد. يمكنك مشاهدة الكلمات الرئيسية المحددة، لمعرفة التغييرات التي تم إجراؤها على مواقع منافسيك.

- **SEMRush**

المصدر: http://www.semrush.com

SEMRush هو موقع ويب للبحث عن الشركات المنافسة. لأي موقع، يمكنك الحصول على قائمة من الكلمات الرئيسية المسجلة لموقع جوجل و**AdWords**، أما هنا يمكنك الحصول على قائمة المنافسين في نتائج بحث جوجل. الوسائل الضرورية لاكتساب المعرفة المتعمقة حول ما يقوم به المنافسين من الدعاية وتخصيص ميزانية لتكتيكات التسويق عبر الإنترنت يتم توفيرها من قبل**SEMRush** .

- **Jobitorial**

المصدر: http://www.jobitorial.com

Jobitorial يسمح للموظفين المجهولين من رؤية ما تم نشره عن الوظائف لآلاف الشركات ويسمح لك أيضا بمراجعة الشركة.

- **AttentionMeter**

المصدر: http://www.attentionmeter.com

AttentionMeter هو أداة تستخدم لمقارنة أي موقع تريده (**traffic**) باستخدام **Alexa**، **compete**، و**QuantCast**. أنها تعطيك لقطة عن حركة البيانات وكذلك الرسوم البيانية من **Alexa**، **Compete**، و**QuantCast**.

- **ABI/INFORM Global**

المصدر: http://www.proquest.com

ABI/INFORM Global هو قاعدة بيانات الأعمال. يقدم أحدث المعلومات التجارية والمالية للباحثين على جميع المستويات. مع **ABI/INFORM Global**، يمكن للمستخدمين تحديد ظروف العمل، تقنيات الإدارة، الاتجاهات التجارية، ممارسة الإدارة ونظرية واستراتيجية وتكتيكات الشركات، والمشهد التنافسي.

- **Compete PRO**

المصدر: http://www.compete.com

Compete PRO يوفر خدمة الاستخبارات التنافسية على الإنترنت. فهو يجمع بين كل موقع، وبحث، وتحليل في منتج واحد.

5-عملية الاستطلاع باستخدام جوجل(FOOTPRINTING USING GOOGLE)

على الرغم من أن جوجل هو عباره عن محرك بحث، فان عملية الاستطلاع (Footprinting) باستخدام جوجل ليست مشابهة لعملية الاستطلاع (Footprinting) من خلال محركات البحث. لقد أثبتت جوجل ليكون واحدا من أفضل وأشمل محركات البحث حتى الآن. حيث أصبح violently spider websites، وذلك لعرضه معلومات حساسة من غير قصد عن موقع ما على شبكة الإنترنت وذلك نتيجة الاعداد الخاطئ لمختلف خوادم/ملقمات الويب (مثل فهرسة الدليل). مثل هذه النتائج تعرض كميات هائلة من البيانات التي تتسرب إلى شبكة الإنترنت، وأسوأ من ذلك، انا هذه النتائج تخزن في google cache. في أوائل عام 2000، أنجب حقل جديد، وهو قرصنة جوجل. قرصنة جوجل [google hack] قدم للمرة الأولى من قبل جوني لونج، الذي نشر بضعة كتب حول هذا الموضوع، مثل كتاب *Google Hacking for Penetration Testers* للكاتب جوني لونج [Johnny Long]. الفكرة العامة وراء قرصنة جوجل هو استخدام معاملات بحث متقدمة في محرك البحث جوجل لتضييق نتائج البحث والعثور على ملفات محددة للغاية، وعادة مع صيغة معروفة. يمكنك أن تجد معلومات الاستخدامات الأساسية هنا:

https://support.google.com/websearch/answer/134479?hl=en

ملحوظه: يقوم جوجل بفلتره الاستخدام المفرط لمشغل البحث المتقدم ويقوم بخفض الطلبات (request)بمساعدة نظام الوقاية من الاختراق.

عملية الاستطلاع باستخدام تقنية قرصنة جوجل FOOTPRINTING USING GOOGLE HACKING TECHNIQUES

قرصنة جوجل (Google Hacking) هو فن إنشاء عمليات بحث معقده من خلال محرك البحث جوجل عن طريق استخدام صيغ معقده (google operator) وذلك للعثور على الثغرات الأمنية في ملفات الإعداد وأكواد الكمبيوتر التي تستخدمها المواقع. إذا استطعت بناء الاستعلامات المناسبة، فانه يمكنك الحصول على بيانات قيمة حول الشركة المستهدفة من نتائج بحث جوجل. من خلال عملية **قرصنة جوجل**، فأن المهاجم يحاول العثور على المواقع التي هي عرضة للعديد من المآثر ومواطن الضعف. هذا يمكن أن يتحقق مع مساعدة من قواعد بيانات قرصنة جوجل (GHDB)، وقواعد البيانات الخاصة بالاستعلام لتحديد البيانات الحساسة. مشغلي جوجل تساعدك في العثور على النص المطلوب وتجنب البيانات التي لا صلة لها بالموضوع. باستخدام مشغل جوجل المتقدم، فأن المهاجمين يمكنهم تحديد موقع جمله محددة من النص مثل إصدارات معينة من تطبيقات الويب الضعيفة.

مشغلي جوجل المتقدم [advanced google operator]:

لحسن الحظ بالنسبة لنا، يوفر جوجل بعض التعبيرات التي هي سهلة الاستخدام والتي تساعدنا في الحصول على أقصى استفادة من عملية البحث. هذه التوجيهات هي الكلمات الرئيسية التي تمكننا من استخراج معلومات أكثر دقة من فهرس جوجل.
مشغلي البحث المتقدم تسمح لك بتضييق عملية البحث الخاص بك حتى تصل الى النقطة التي يتم فيها تحديد الهدف الذي كنت تبحث عنه بالضبط، ويمكن الاطلاع على قائمة مشغلي جوجل في جوجل:

http://support.google.com/websearch/bin/answer.py?hl=en&answer=136861

باستخدام هذه العوامل، يمكنك البحث عن المعلومات المحددة التي قد تكون ذات قيمة خلال اختبار الاختراق. دعونا نحاول في بعض الأمثلة البسيطة للحصول على نتائج دقيقه.

النظر في المثال التالي: افترض أنك تبحث عن معلومات عن موقع جامعة ولاية داكوتا (dsu.edu) عن شخص ما. أبسط طريقة لأداء هذا البحث هو إدخال المصطلحات التالية (بدون أي علامات اقتباس) في مربع البحث جوجل: [pat engebretson dsu] هذا البحث سوف يسفر عن عدد لا بأس به من النتائج. لكن تجد من خلال اول 50 نتيجة بحث يوجد أربعة نتائج فقط تم انتشالها من موقع (dsu.edu) مباشرة. من خلال الاستفادة من **مشغلي جوجل** (**توجيهات**"directive")، فنحن يمكن أن نجبر مؤشر جوجل للقيام بالعطاءات التي نريدها. في المثال أعلاه نحن نعرف كل من الموقع الهدف والكلمات الرئيسية التي نريد البحث عنها. بشكل أكثر تحديدا، نحن مهتمون بإجبار جوجل بالعودة بالنتائج الوحيدة التي يتم سحبها مباشرة من الموقع الهدف(dsu.edu) . في هذه الحالة، أفضل خيار لدينا هو الاستفادة من التوجيه/التعبير [site:]. باستخدام هذا التعبير فنحن نجبر جوجل على العودة فقط بالنتائج التي تحتوي على الكلمات الرئيسية التي استخدمناها وتأتي مباشرة من الموقع المحدد.

لاستخدام توجيهات/مشغلي جوجل بشكل صحيح، تحتاج إلى ثلاثة أشياء:

1. اسم التوجيه الذي تريد استخدامه.
2. القُولون (:).
3. المصطلح الذي تريد استخدامه في التوجيه.

بعد إدخال الثلاث قطع من المعلومات الواردة أعلاه، يمكنك البحث كما تفعل عادة. لاستخدام التوجيه "site:"، فنحن بحاجة إلى إدخال ما يلي في مربع بحث جوجل:

site:dsu.edu pat engebretson

نلاحظ أنه لا توجد مسافة بين التوجيه والقُولون، واسم الدومين. في مثالنا السابق أردنا إجراء بحث عن **pat engebretson** في موقع الويب [**dsu.edu**]. لإنجاز هذا، فإننا أدخل الأمر السابق في شريط البحث جوجل.

ماذا يمكن أن يفعل الهاكر مع استخدام قرصنة جوجل؟

إذا كان الموقع المستهدف هو عرضة للقرصنة جوجل، فان المهاجم يجد المعلومات التالية مع مساعدة من الاستعلامات في قاعدة بيانات قرصنة جوجل:

- رسائل الخطأ التي تحتوي على معلومات حساسة
- الملفات التي تحتوي على كلمات السر
- المجلدات الحساسة
- الصفحات التي تحتوي على بوابات الدخول
- الصفحات التي تحتوي على بيانات الشبكة أو الضعف
- تحذيرات ونقاط الضعف الخادم

عمليات البحث المتقدم لمشغلي جوجل GOOGLE ADVANCE SEARCH OPERATORS

المصدر: **http://www.googleguide.com**

[cache:] استعلام **cache** يعرض نسخة جوجل (**Google's cached version**) من صفحة الويب، بدلا من الإصدار الحالي من الصفحة. بمعنى اخر للحد من نتائج البحث ويظهر المعلومات فقط التي سحبت مباشرة من ذاكرة التخزين المؤقت لجوجل.

على سبيل المثال: (**cache:www.eff.org**).

ملاحظة: لا تضع مسافة بين عنوان URL وبين (cache:).

[link:] يعمل **link** على سرد صفحات الويب التي تحتوي على الروابط المحددة لصفحة الويب. على سبيل المثال، للبحث عن الصفحات التي تشير إلى الصفحة الرئيسية ل **Google Guide's**، أدخل الاتي: (**link:www.googleguide.com**). هذا يعنى أنه سوف يسرد لك جميع صفحات الويب الذي تحتوي على لنكات او روابط للموقع **www.googleguide.com**.

ملاحظة: ووفقا لتوثيق غوغل، "لا يمكنك الجمع بين بحث (**link:**) مع كلمات البحث العادية. نلاحظ أيضا أنه عند الجمع بين(**link:**) مع معاملات البحث المتقدم الأخرى، فان جوجل قد لا ترجع كافة الصفحات التي تتطابق. الاستعلامات التالية يجب أن تعود بالكثير من النتائج، إذا قمت بإزالة المعامل (**-site:**) من هذه الاستعلامات.

[related:] إذا قمت بتشغيل الاستعلام الخاص بك مع " **related:** " ، فان جوجل يعرض المواقع المماثلة إلى الموقع المذكور في استعلام البحث. مثال: (**related:www.microsoft.com**) سيوفر نتائج محرك البحث جوجل المواقع المشابهة لموقع **microsoft.com.**

[info:] سوف يقدم لك بعض المعلومات عن صفحة الويب. على سبيل المثال،(**info:gothotel.com**) سوف تظهر معلومات حول دليل الفنادق للصفحة الرئيسية **GotHotel.com**.

ملاحظة: يجب ألا يكون هناك مسافة بين (info:) و URLصفحة ويب .كما يمكن الحصول على هذه الوظيفة عن طريق كتابة URL في صفحة الويب مباشرة في مربع البحث جوجل.

[site:] إذا قمت باستخدام (**site:**) في الاستعلام الخاص بك ، فان جوجل سوف تعمل على تقييد نتائج البحث للموقع أو الدومين الذي تحدده. على سبيل المثال، (**site:www.lse.ac.uk**) هذا سوف يظهر لك معلومات القبول في كلية لندن للاقتصاد و [**peace site:gov**] سوف يجد الصفحات عن السلام داخل الدومين (**.gov**). يمكنك تحديد الدومين مع أو بدون **period**، على سبيل المثال، إما (**.gov**) أو (**gov.**) ملاحظة: لا تتضع مسافة بين " **site:**" والدومين.

[allintitle:] إذا قمت بتشغيل الاستعلام الخاص بك مع **allintitle** ، فان جوجل يقيد النتائج إلى تلك التي تحتوي على كل شروط الاستعلام الذي تم تحديده في العنوان.

على سبيل المثال،(**allintitle: detect plagiarism**) فان هذا سوف يعود بالوثائق الوحيدة التي تحتوي على الكلمات **detect** و**plagiarism** في العنوان. كما يمكن الحصول على هذه الوظيفة من خلال صفحة الويب للبحث المتقدم، ضمن **Occurrences**.

[intitle:] على سبيل المثال (**intitle:term**) فان هذا سوف يقيد النتائج إلى المستندات التي تحتوي على المصطلح **term** في العنوان.

ملحوظة: يجب ألا يكون هناك مسافة بين **intitle:** والكلمة التالية.

[allinurl:] إذا قمت بتشغيل الاستعلام الخاص بك مع **allinurl:** فان جوجل يقيد النتائج إلى تلك التي تحتوي على كل مصطلحات الاستعلام الذي تحدده في**URL** .

على سبيل المثال، (allinurl: google faq) فان هذا سوف يعود إليك بالوثائق الوحيدة التي تحتوي على الكلمات "google" و" faq " في عنوان URL ، مثل(www.google.com/help/faq.html) هذه الوظيفة يمكن أيضا الحصول عليها من خلال صفحة الويب للبحث المتقدم، ضمن الحوادث(Occurrences).

في عناوين المواقعURL، غالبا ما يتم تشغيل الكلمات معا. ولكن لا تحتاج أن تدار معا عندما تستخدم allinurl.

[inurl:] إذا قمت بتضمينinurl في طلب الاستعلام الخاص بك ، فان جوجل سوف تقييد النتائج إلى المستندات التي تحتوي على تلك الكلمة في عنوانURL .

على سبيل المثال، (inurl:print site:www.googleguide.com) فان هذا سوف يبحث عن الصفحات في موقع googleguide على العنوانين التي تحتوي على كلمة " print ". إنها تجد ملفات PDF التي هي في الدليل أو في المجلد المسمى " print " على موقع الويب googleguide. [inurl:healthy eating] أن عملية الاستعلام هذه سوف تعود إليك بالوثائق التي تحتوى على الكلمة healthy في عنوانها والتي تحتوى على الكلمة eating في أي مكان داخل الوثيقة.

ملحوظه: لا يوجد مسافة بين المصطلح :inurl والكلمة التي تليها.

[filetype:] يمكننا الاستفادة من هذا التوجيه في البحث عن ملف معين داخل مواقع الويب. هذا مفيد للغاية للعثور على أنواع معينة من الملفات على موقع الويب الخاصة بالهدف. على سبيل المثال، للعودة الفاعلية بالنتائج الوحيدة التي تحتوي على وثائق PDF، ويوجد تعبير اخر مشابه له وهو [ext:] بحيث يوضع بعده الامتداد المطلوب البحث عنه. ونستخدم التعبير التالي:

ext:pdf filetype:pdf

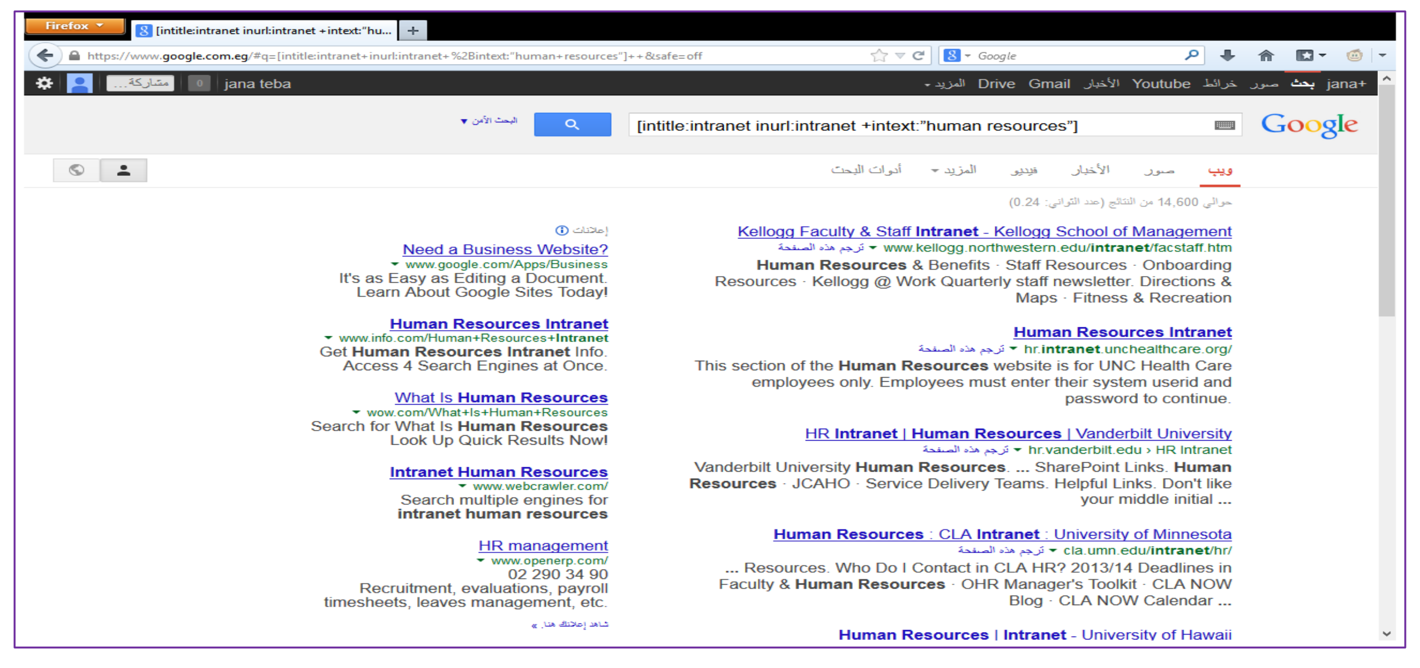
[intext:] هذه تفيد الى تقيد نتائج البحث بحيث المحتوى المعروض يكون يحتوى على الكلمات الرئيسية الموجودة في txt.

هناك العديد من أنواع التوجيهات الأخرى الخاصة بقرصنة جوجل التي يجب عليك أن تصبح معتادا عليها. جنبا إلى جنب مع جوجل، فمن المهم أن تصبح فعالة مع العديد من محركات البحث الأخرى أيضا. في كثير من الأحيان، فأن محركات البحث المختلفة تعطي نتائج مختلفة، حتى عند البحث عن نفس الكلمات الرئيسية. تجدر الإشارة إلى أن عمليات البحث هذه تكون في الوضع Passive Footprinting فقط طالما كنت تبحث عنه. بمجرد إجراء اتصال مع النظام الهدف (من خلال النقر على أي من الروابط)، تعود إلى الوضع active. يجب ان تكون على علم بأن استطلاع الأنشطة دون إذن مسبق من المرجح أنه غير قانوني.

إيجاد الموارد باستخدام عمليات جوجل للبحث المتقدم FINDING RESOURCES USING GOOGLE ADVANCE OPERATOR

باستخدام تعبيرات جوجل المتقدمة مثل [intitle:intranet inurl:intranet +intext:"human resources"] فان المهاجم يمكنه العثور على معلومات خاصة عن الشركة المستهدفة وفى بعض الأحيان معلومات حساسة حول موظفي تلك الشركة بالذات. المعلومات التي تم جمعها من قبل المهاجمين يمكن استخدامها لتنفيذ هجمات الهندسة الاجتماعية. إن محرك جوجل سوف يعمل على فلترة الاستخدام المفرط للمشغل البحث المتقدم وسوف ينخفض الطلبات بمساعدة نظام منع الاختراق.

الشكل التالي يظهر صفحة نتائج محرك البحث جوجل المتقدم بعرض نتائج الاستعلام التي سبق ذكرها:



بمجرد الوصول الى صفحة الويب الهدف عن طريق إجراء عمليات تفتيش شاملة باستخدام جوجل ومحركات البحث الأخرى، فمن المهم استكشاف زوايا أخرى من الإنترنت. مجموعات الأخبار ونظام لوحة الاعلانات [Bulletin Board Systems (BBS)]مثل UseNet و Google Group يمكن أن تكون مفيدة جدا في جمع المعلومات عن الهدف.

ملحوظه: نظام لوحة الاعلانات [Bulletin Board Systems (BBS)] هو نظام حاسوبي يعمل من خلاله برنامج يُمكن المستخدمين من الاتصال والدخول إلى النظام باستخدام المحطة الطرفية. عند الدخول إلى النظام، يستطيع المستخدم تنفيذ عمليات مثل تحميل وارسال البرامج أو البيانات كذلك يستطيع المستخدم قراءة الأخبار والنشرات وتبادل الرسائل مع المستخدمين الاخرين.

ليس من المألوف للناس استخدام مجالس المناقشة هذه لإرسال وتلقي المساعدة في المسائل التقنية. للأسف (أو لحسن الحظ، اعتمادا على أي جانب من العملة تبحث فيها)، حيث في كثير من الأحيان يقوم الموظفين بإضافة أسئلة مفصلة جدا بما في ذلك المعلومات الحساسة والسرية. على سبيل المثال، ضع في الاعتبار مسؤول الشبكة [admin]الذي وجود صعوبة في إعداد جدار الحماية بشكل صحيح. حيث ليس من المألوف أن تشهد في المناقشات في المنتديات العامة حيث سيتم نشر ملفات الاعداد الخاصة بهم. لجعل الأمور أسوأ، وكثير من الناس يقوموا باستخدام عناوين البريد الإلكتروني الخاصة بالشركة التي يعملون بها. هذه المعلومات هو منجم ذهب بالنسبة للمهاجمين. حتى لو كان مشرف الشبكة هذا يتميز بالذكاء والحرص بما فيه الكفاية عن طريق عدم نشر ملفات الاعداد الخاصة بهم، حيث إنه من الصعب الحصول على دعم من المجتمع دون تسرب بعض المعلومات دون قصد. لذلك سوف تقرأ بعناية المشاركات الخاصة به [posts] التي كثيرا ما تكشف إصدار محدد من البرمجيات، ونماذج الأجهزة ومعلومات الاعداد الحالي، وما شابه ذلك حول الأنظمة الداخلية. يجب تقديم كل هذه المعلومات بعيدا لاستخدامها في المستقبل.

المنتديات العامة هي وسيلة ممتازة لتبادل المعلومات والحصول على المساعدة التقنية. ومع ذلك، عند استخدام هذه الموارد، يجب ان تتوخى الحذر وذلك عن طريق استخدام عناوين البريد الإلكتروني المجهولة مثل Gmail أو هوتميل، بدلا من عنوان الشركة.

النمو الهائل في وسائل الاعلام الاجتماعية مثل الفيس بوك، ماي سبيس، وتويتر يوفر لنا آفاقا جديدة لبيانات الألغام حول أهدافنا. عند تنفيذ الاستطلاع، فإنها فكرة جيدة لاستخدام هذه المواقع لصالحنا. النظر في المثال التالي: تقوم بإجراء اختبار الاختراق ضد شركة صغيرة. وقد أدى هذا الاستطلاع ليكشف لك أن مسؤول الشبكة للشركة لديه حساب تويتر وفيسبوك.

مع الاستفادة من الهندسة الاجتماعية فيمكنك اقامة علاقات صداقة معهم وتقوم بتتبعهم على حد سواء في الفيسبوك وتويتر. بعد بضعة أسابيع من المشاركات المملة، يحدث انه يكتب مثلا على الفيسبوك " الجدار الناري توفي دون سابق إنذار اليوم. وواحدة جديدة يتم إعدادها خلال الليل. يبدو أنني سوف اجلس الليل كله لإعادة الأمور إلى وضعها الطبيعي". ومثال آخر " انتهيت للتو من عملية الميزانية السنوية. يبدو أنى عالق مع خادم server 2000 لمدة عام آخر". من هذا نرى كمية المعلومات التي يمكن أن نجمعها ببساطة عن طريق رصد ما تم نشره من قبل الموظفين على الانترنت.

ما هو اليوزنت " USENET "

الجدير بالذكر ان المنتديات والشبكات الاجتماعية الموجودة الان والمنتشرة بشكل كبير وواسع ما هي الا تطوير وتحديث لتلك التقنية العبقرية. كانت هذه الفكرة من بنات افكار الشباب توم تراسكوت وجيم ايليس خريجي جامعة ديوك وظهرت للعالم سنة 1980

لكن ما هو اليوزنت وما فائدته؟ تستطيع ان تقوم بإضافة مقالات وتعليقات في مجتمع او شبكة اليوزنت وهو ما يسمى بشكل عام الاخبار فكل مقال في شبكة اليوزنت هو عبارة عن خبر ويتم تصنيفه على شكل تصنيفات او اقسام تسمى مجموعات الاخبارnewsgroups . تعد اليوزنت من أقدم شبكات الحاسوب والاتصالات وما زالت موجودة حتى الان وقد ظهرت قبل ظهور الشبكة العالمية وانتشارها بحوالي عشرة سنوات تقريبا. ولكن ما هي newsgroups او مجموعات الاخبار؟ هي بكل بساطة مجموعات نقاش مثل المنتديات التي تستخدم للنقاش بين الاعضاء من مختلف الاماكن الموجودة الان على الشبكة العالمية. تقسم مجموعات الاخبار تلك الى ثماني مجموعات رئيسية تسمىBig Eight . وليس معنى هذا عدم وجود مجموعات اخرى، بل يوجد مجموعات اخرى بلغات مختلفة غير الانجليزية وايضا يوجد مجموعة اخرى تسمىalt .وسأقوم بعرض تلك المجموعات الثمانية وتعريف لكل واحدة على حدة.

Comp: تهتم تلك المجموعة بالمواضيع الخاصة بالكمبيوتر من برامج وغيرها.

Humanities: تهتم بالأدب والفلسفة والتصميمات أي انها مجموعة متخصصة في الفن.

Misc: هذه المجموعة ليس لها شيء محدد فهي تهتم بمواضيع متنوعة عن التعليم والاطفال وغيرها.

News: كما نفهم من اسمها فهي تهتم بالأخبار ولكن ليست اخبار عادية فهي تهتم بأخبار النقاشات والاحداث الجديدة عن المجموعات.

Rec: خاصة بالتسلية والترفيه من افلام ومسلسلات.

Sci: تضم النقاشات الخاصة بالعلوم والابحاث العلمية.

Soc: الاجتماعيات والثقافات المختلفة الموجودة في المجتمع.

Talk: تضم نقاشات حول السياسة والدين والمنشئ.

قرصنه جوجل: قاعدة بيانات قرصنة جوجل (GHDB) (GOOGLE HACKING DATABASE)

المصدر: **http://www.hackersforcharity.org**

هناك المئات (إن لم يكن الآلاف) من عمليات البحث مثيره للاهتمام التي يمكن تقديمها. يتم سرد العديد منهم في قسم "قرصنة جوجل " في قاعدة بيانات**Exploit**. **GHDB** تعمل على تنظيم عمليات البحث في فئات مثل **Username** و **password**، وحتى على حسب معدلات البحث كل شهر. يرجى أخذ الوقت الكافي لزيارة هذا الموقع، وإذا كان هذا الموضوع مثير بالنسبة لك (فأنه ينبغي!)، النظر في كتاب **Google Hacking for Penetration Testers** الطبعة الثانية.

قاعدة بيانات قرصنة جوجل (**GHDB**) هي قاعدة بيانات تحتوي على عدد كبير من الاستفسارات (تعبيرات الاستعلام) التي تحدد البيانات الحساسة. **GHDB** هو تطبيق مجمع بين **HTML/جافا سكريبت** التي تستخدم تقنيات متقدمة من الجافا سكريبت والتي أنشئت من قبل **Johnny Long** (قرصان للأعمال الخيرية)، ويوجد في [**http://www.hackersforcharity.org/ghdb/**].

Offensive Securityيحتوى هو الاخر على **GHDB** في

http://www.offensive-security.com/community-projects/google-hacking-database/

لقد تم الدمج بين GHDB مع قاعدة بيانات Exploit. (EDB)Exploit database –(http://www.exploit-db.com) .

العثور على نقاط الضعف في الخوادم/السيرفرات عن طريق جوجل

كل بضعة أيام، توجد نقاط ضعف لتطبيق ويب جديده. كثيرا ما يمكن استخدام جوجل لتحديد الخوادم/السيرفرات الضعيفة. على سبيل المثال، في فبراير 2006، تم العثور على ثغرة في **phpBB** (منتدى مفتوح المصدر للبرمجيات). فقامت القراصنة باستخدام جوجل للتعرف على وجه السرعة على جميع المواقع الموجودة على شبكة الإنترنت التي تستخدم **phpBB** لاستهدافها. قراءة المزيد عن الضعف / استغلال هنا:
http://www.exploit-db.com/exploits/1469/

"Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"



الأدوات الأخرى المستخدمة في قرصنة جوجل

بجانب استخدام أداة قواعد بيانات قرصنة جوجل (GHDB)التي تم ذكرها في السابق، فان هناك بعض الأدوات الأخرى التي يمكن أن تساعدك مع قرصنة جوجل. هناك عدد من أكثر أدوات قرصنة جوجل المذكورة على النحو التالي. باستخدام هذه الأدوات، يمكن المهاجمين جمع التحذيرات ونقاط الضعف لخادم ما، معلومات رسالة الخطأ التي قد تكشف عن مسارات الهجوم للملفات الحساسة، الأدلة، بوابات الدخول [**gateway**]، وأكثر من ذلك.

ملحوظه: محرك البحث جوجل لا يسمح بتطبيق عملية البحث باستخدام التطبيقات المختلفة لذلك عند استخدام هذه التطبيقات يرجى تحديثها اما بنج فلا يمنع ذلك.

- **Metagoofil**

المصدر:**http://www.edge-security.com**

Metagoofil هو أداة لجمع المعلومات مصممة لاستخراج البيانات الوصفية (**metadata**) من الوثائق العامة التابعة للشركة الهدف.

(Pdf, doc, xls, ppt, docx, pptx, xlsx)

Metagoofil ينفذ عملية البحث في جوجل لتحديد وتحميل المستندات إلى القرص المحلي ثم استخراج البيانات الوصفية عن طريق ملفات المكتبات المختلفة (**libraries**) مثل **Hachoir**، **PdfMiner?** ، وغيرها. مع النتائج، فإنه يولد تقريرا يتضمن أسماء المستخدمين، إصدارات البرامج، والخوادم أو أسماء الآلة التي قد تساعد في اختبار الاختراق في مرحلة جمع المعلومات.

- **Goolink Scanner**

المصدر: **http://www.ghacks.net**

Goolink Scanner يزيل ذاكرة التخزين المؤقت (**cache**) من عمليات البحث الخاصة بك، ويجمع و يعرض روابط الموقع التي تحتوى على نقاط ضعف فقط. وبالتالي، فإنه يسمح لك لإيجاد المواقع المعرضة للخطر مفتوحة على مصراعيها ل **google** و**googlebots**.

- **SiteDigger**

المصدر: **http://www.mcafee.com**

SiteDigger يبحث في الذاكرة الموقتة لجوجل (Google's cache) ليجد نقاط الضعف ، والأخطاء ، وقضايا الإعداد والمعلومات الشخصية، و شذرات الأمن المثيرة للاهتمام على مواقع الإنترنت.

- **Google Hacks**

المصدر: **http://code.google.com**

Google Hacks هو تجميع لعمليات بحث جوجل التي تعرض أدوات جديده من خدمات البحث وخريطة جوجل. فإنه يسمح لك برؤية الجدول الزمني لنتائج البحث الخاصة بك، عرض الخريطة، البحث عن الموسيقى، البحث عن الكتب، تنفيذ العديد من أنواع أخرى محددة من عمليات البحث.

- **BILE Suite**

المصدر: **http://www.sensegost.com**

BILE Suite من اجل **Bi-directional Link Extractor**. يشمل **BILE Suite** بضع من سكريبات برل المستخدمة في عمليات التعداد. كل مخطوطة من سكريبات برل لديه وظيفة خاصة بها. **BiLE.pl** هو الأداة الأولى أو مجموعة سكريبات بيرل. **BiLE** يميل على جوجل وHTTrack يستخدم لجمع أليا من وإلى الموقع المستهدف ، ثم تطبيق الخوارزميات البسيطة للاستدلال على المواقع التي تملك أقوى العلاقات مع الموقع المستهدف.

- **Google Hack Honeypot**

المصدر: **http://ghh.sourceforge.net**

Google Hack Honeypot (GHH) هو رد فعل لنوع جديد من **malicious web traffic: search engine hackers**. هي مصممة لتوفير عمليات الاستطلاع ضد المهاجمين الذين يستخدمون محركات البحث كأداة قرصنة ضد الموارد الخاصة بك. **GHH** تعمل على تطبيق نظرية المصيدة (**honeypot theory**) لتوفير أمان إضافي إلى شبكة الإنترنت الخاصة بك.

- **GMapCatcher**

المصدر: **http://code.google.com**

GMapCatcher هو **offline maps viewer**. فإنه يعرض خرائط للعديد من مزودي الخدمة مثل: **CloudMade**، **OpenStreetMap**، **Yahoo Maps**، **Bing Maps**، **Nokia Maps**، و**Skyvector**. (**maps.py**) هو برنامج واجهة المستخدم الرسومية المستخدمة لتصفح خريطة جوجل. مع الزر **offline toggle** بإزالة الإشارة من عليه (عدم تفعيله)، فإنه يمكن تحميل خريطة جوجل تلقائيا. بمجرد تحميل الملف، فإنه يصبح موجود على القرص الثابت. وبالتالي، لا تحتاج لتحميل البرنامج مرة أخرى.

- **SearchDiggity**

المصدر: **http://www.stachliu.com**

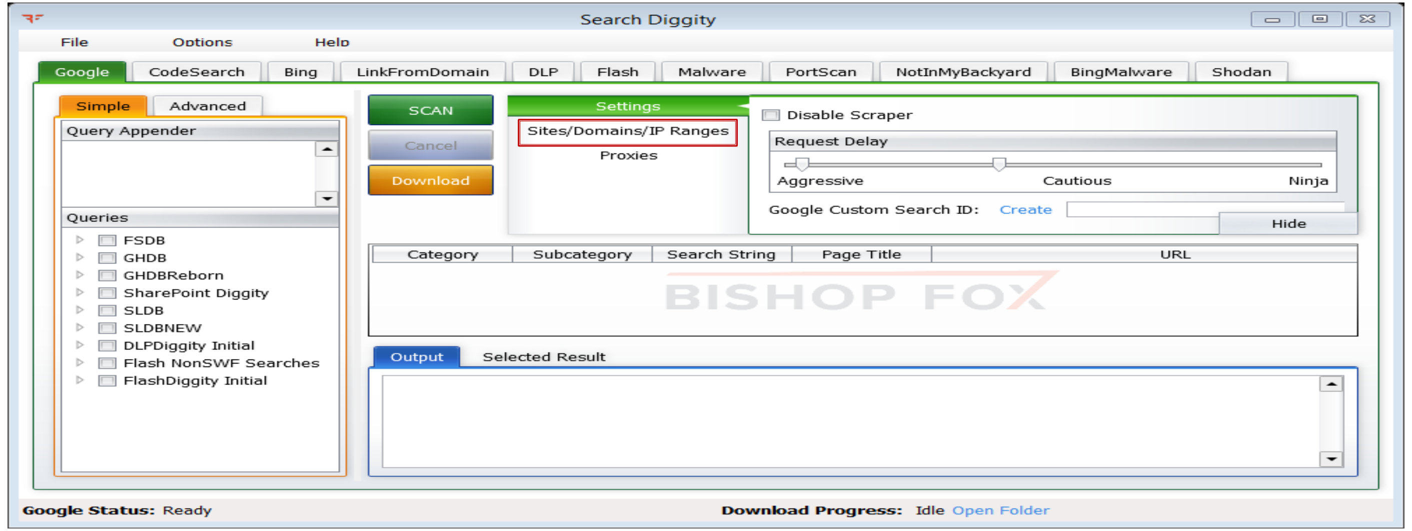
SearchDiggity هو أداة الهجوم الرئيسي للمشروع **Google hacking Diggity**. هو عباره عن **Stach** وتطبيق **Liu's**ذات واجه رسوميه لمايكروسوفت التي هي بمثابة الواجهة الأمامية لأحدث الإصدارات من أدوات **Diggity** مثل **GoogleDiggity**، **Bing**،**BingDiggity** ، **LinkFromDomainDiggity**، **CodeSearchDiggity**، **DLPDiggity**، **MalwareDiggity**، **PortScanDiggity**، **SHODANDiggity**، **BingBinaryMalwareSearch**، و **NotInMyBackYard Diggity**.

ملحوظه: يعتبر هذا الموقع من المواقع التي تعطى أدوات وخبرات في عمليات القرصنة

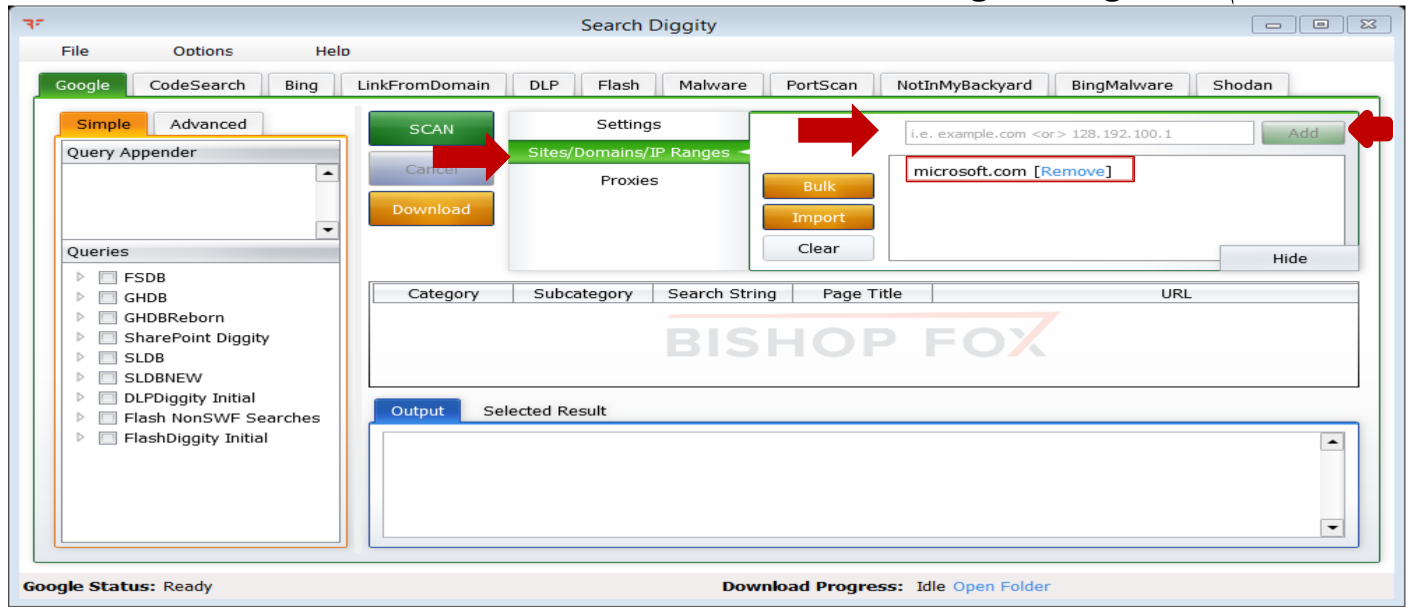
من الطرق السهلة لإيجاد ثغرات المواقع الإلكترونية والتطبيقات هو استخدام جوجل والذي يعتبر من الأدوات السهلة بالنسبة للمهاجم. باستخدام اكواد جوجل في البحث فانه يمكن المهاجم من إيجاد الثغرات في ملف الكود الخاص بتطبيق معين والذي يدعمه بنقطة الدخول الذي يحتاجها لتنفيذ عملية الاختراق واختراق الوضع الأمني لهذا التطبيق. بما إنك هاكر أخلاقي فإنه يجب عليك استخدام نفس التطبيق لإيجاد الثغرات ثم صنع باتش لمعالجة مثل هذه الثغرات.

1- يتم تثبيت البرنامج عن طريق **wizard** الخاص به

2- ثم يتم تشغيله فتظهر الشاشة التالية ونلاحظ انها في الوضع الافتراضي وهو **google**:



3- نختار التعيين **Sites/Domains/IP Ranges** فيظهر مربع حواري ندخل فيه اسم الدومين وليكن مثلا Microsoft.com ثم نضغط على **add** كالاتي:



4- ثم بعد ذلك نذهب الى القائمة الموجودة في الجانب الايسر واختيار نوع الطلب الذي تريد البحث عن وليكن مثلا **FlashDiggity Initial** ثم نختار **SWF Finding Generic** ثم نضغط **SCAN** فتظهر ناتج البحث وهو عباره عن جميع عناوين **URL** في الدومين **microsoft.com** والتي تحتوي على ملفات **SWF**.

- **Google HACK DB**

المصدر: **http://www.secpoint.com**

يمكن للمهاجم أيضا استخدام الأداة **SecPoint Google HACK DB** لتحديد المعلومات الحساسة عن موقع الهدف. هذه الأداة تساعد المهاجم على استخراج الملفات التي تحتوي على كلمات السر، ملفات قواعد البيانات، ملفات نصية واضحة، ملفات قاعدة بيانات العملاء، وما إلى ذلك.

- **Gooscan**

المصدر: **http://www.darknet.org.uk**

Gooscan هو أداة تعمل على إنشاء استفسارات بطريقه أليه ضد تطبيق بحث جوجل. وقد صممت هذه الاستعلامات للعثور على الثغرات المحتملة على صفحات الويب.

- **محركات البحث الأخرى**

من الواضح أن هناك محركات بحث أخرى وبصرف النظر عن جوجل. يمكنك الاطلاع على قائمة لطيفة من محركات البحث الأخرى وقدرات بحثهم من خلال هذا الرابط:

http://www.searchengineshowdown.com/features/

يوجد محرك بحث الذي استولت وظيفة على انتباهي وهي قدرات البحث عن عناوين الـ **IP** وهذا المحرك هو **gigablast.com**. يمكن أن تبحث عن محتوى على شبكة الإنترنت من خلال عنوان **IP**. هذا يساعد في تحديد **load balancer**، دومين إضافي، وهلم جرا. اكتشفت مؤخرا أن محرك البحث **MSN** يدعم هو الاخر قدرات البحث عن عناوين الـ **IP** عن طريق استخدام الصيغة [**ip:search_word**].

6-عمليات الاستطلاع باستخدام WHOIS (WHOIS FOOTPRINTING)

جمع المعلومات المتعلقة بالشبكة مثل معلومات **WHOIS** عن موقع المنظمة المستهدفة يعتبر مهم جدا عند قرصنة النظام. لذلك، والآن سوف نناقش عمليات الاستطلاع باستخدام **WHOIS**.

يركز **WHOIS Footprinting** حول كيفية إجراء بحث **WHOIS**، وتحليل نتائج البحث، والأدوات اللازمة لجمع إحصائيات عن موقع.

بحثWHOIS (WHOIS LOOKUP)

WHOISهو بروتوكول استعلام و استجابة. يستخدم للاستعلام عن بيانات المستخدمين المسجلين أو موارد الإنترنت المسجلة ، مثل اسم الدومين ، عنوان IP ، أو نظام الحكم الذاتي.

WHOIS هو عباره عن قواعد بيانات أنشأت بواسطة مهندسي الشبكة المحلية وتحتوى على معلومات شخصيه عن أصحاب الدومين. تتم المحافظة على قواعد بيانات **WHOIS** من قبل سجلات الإنترنت الإقليمية. أنها تحتفظ بسجل يسمى **جدول البحث (LOOKUP table)** الذي يحتوي على كافة المعلومات المرتبطة بالشبكة، الدومين والعميل (**host**). يمكن لأي شخص الاتصال والاستعلام من قبل هذا الخادم (**server**) للحصول على معلومات عن الشبكات، على وجه الخصوص، الدومين، والمضيفين(**hosts**). يتم الاشراف على قاعدة بيانات السجل المركزي لـ **whois**بواسطة **InterNIC**. وعادة ما يتم نشر هذه البيانات من قبل خادم الإحصائيات **whois** عبر منفذ **TCP 43** والتي يمكن الوصول إليها باستخدام برنامج **whois**.

يمكن للمهاجم إرسال استعلام إلى خادم **WHOIS** للحصول على المعلومات حول اسم الدومين المستهدف، وتفاصيل الاتصال عن صاحبها وتاريخ انتهاء الصلاحية، وتاريخ الإنشاء، وما إلى ذلك. خادم **WHOIS** سيستجيب إلى الاستعلام عن المعلومات ذات الصلة. كل هذه المعلومات يمكن استخدامها لمواصلة عملية جمع المعلومات أو لبدء هجوم الهندسة الاجتماعية.

Whois يمكنه أيضا تنفيذ عمليات البحث العكسي. بدلا من إدخال اسم النطاق/الدومين، يمكنك إدخال عنوان IP. وسوف تشمل عادة نتيجة **whois** نطاق الشبكة بأكملها الذي ينتمي إلى المنظمة.

المعلومات التي يوفرها لك WHOIS كالاتي:

- اسم الدومين بالتفصيل.
- بيانات الاتصال لصاحب الدومين.
- أسماء سيرفرات الدومين.
- نطاق الشبكة **NETRANGE**.
- المكان الذي أنشاء فيه الدومين.
- أخر السجلات التي تم تحديثها فيه.

المؤسسات التي تعمل على إنشاء WHOIS (Regional Internet Registries(RIRs))

LACNIC **APNIC** **AFRINIC** **ARIN**

تحليل نتائج WHOIS LOOKUP

WHOIS Lookup يمكن القيام به باستخدام خدمات **Whois** على شبكة الانترنت مثل **http://whois.domaintools.com** أو **http://centralops.net/co** أو **http://www.networksolutions.com/whois/index.jsp** أو **http://www.ripe.net** او **.http://www.whois.sc** هنا يمكنك أن ترى ناتج تحاليل نتيجة **WHOIS Lookup** والتي تم الحصول عليها من خلال اثنين من خدمات **WHOIS** المذكورة سابقا. كل من هذه الخدمات تسمح لك بأداء **WHOIS Lookup** عن طريق إدخال اسم الدومين الهدف أو عنوان IP. خدمة **domaintools.com** توفر لك معلومات **WHOIS** مثل معلومات التسجيل، البريد الإلكتروني، معلومات الاتصال الخاصة بالإداريين **(ADMIN)**، تاريخ الإنشاء وانتهاء الصلاحية، قائمة بسيرفرات الدومين، وما إلى ذلك.
ملفات الدومين المتوفرة في **http://centralops.net/co/** يعطي لك معلومات مثل عنوان البحث و domain WHOIS record و network WHOIS record، وسجلات معلومات DNS.

```
Whois Record   Site Profile   Registration   Server Stats   My Whois

Registrant:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329

    Domain Name: microsoft.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329
    Technical Contact, Zone Contact:
        MSN Hostmaster
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

    Created on..............: 1991-05-01.
    Expires on..............: 2021-05-02.
    Record last updated on..: 2011-08-14.

    Domain servers in listed order:

    ns5.msft.net
    ns4.msft.net
    ns1.msft.net
    ns3.msft.net
    ns2.msft.net
```

http://whois.domaintools.com

```
Domain Dossier  Investigate domains and IP addresses

domain or IP address  juggyboy.com
[x] domain whois record   [x] DNS records   [ ] traceroute
[x] network whois record  [ ] service scan  go

   user: anonymous [ 30]
balance: 47 units
         log in | account info                    CentralOps.net

Address lookup
canonical name  juggyboy.com.
       aliases
     addresses  6

Domain Whois record
Queried whois.internic.net with "dom juggyboy.com"...

   Domain Name: JUGGYBOY.COM
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com/en_US/
   Name Server: NS19.WORLDNIC.COM
   Name Server: NS20.WORLDNIC.COM
   Status: clientTransferProhibited
   Updated Date: 03-feb-2009
   Creation Date: 16-jul-2002
   Expiration Date: 16-jul-2014

>>> Last update of whois database: Thu, 19 Jul 2012 07:49:36 UTC <<<

Queried whois.networksolutions.com with "juggyboy.com"...

Registrant:
```

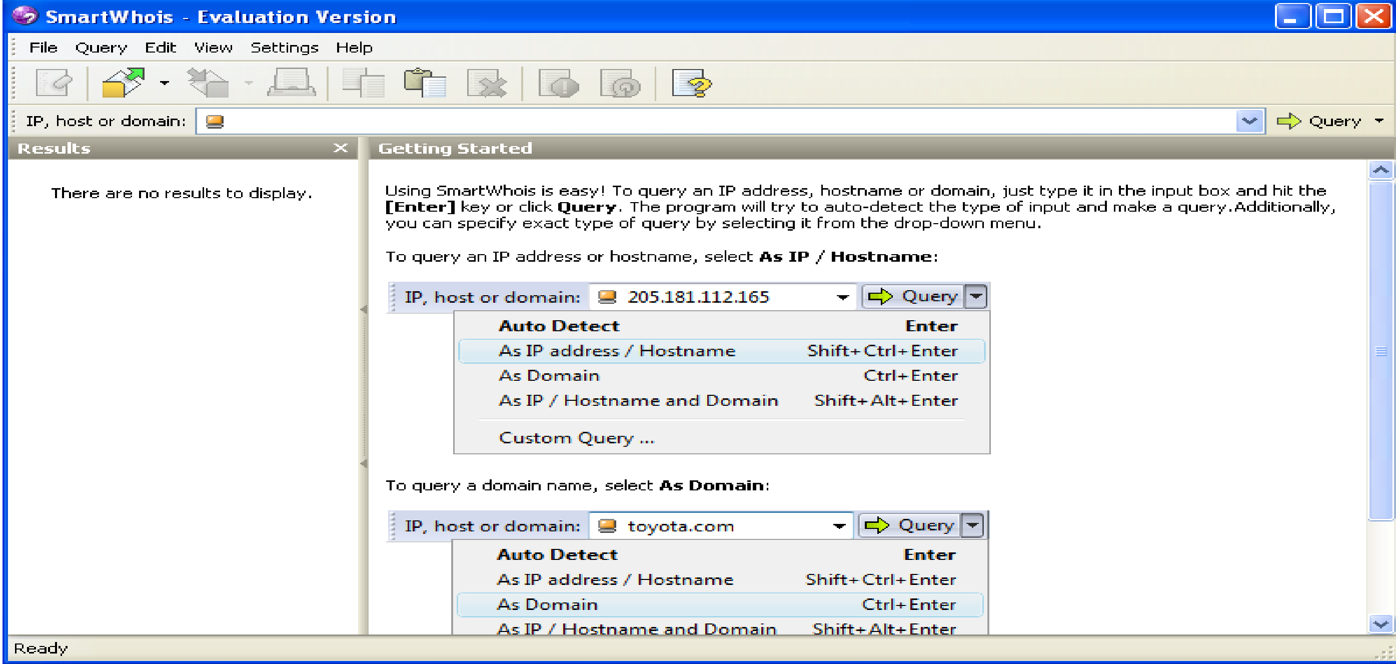
http://centralops.net/co

أدوات WHOIS LOOKUP: (SMARTWHOIS)

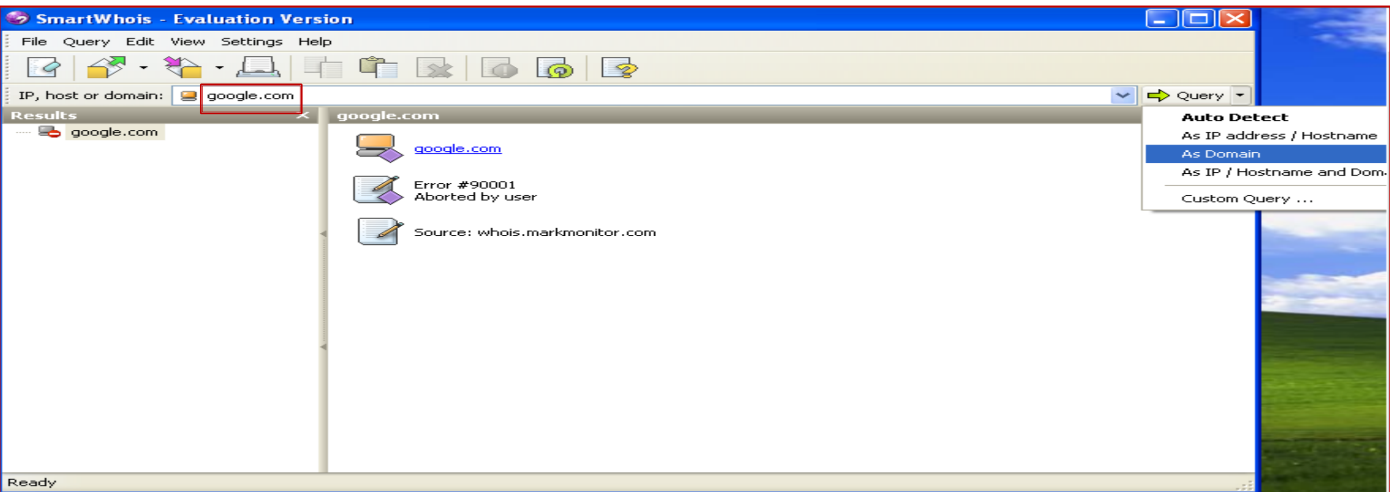
المصدر: **http://www.tamos.com**

SmartWhois هو عبارة عن أداة لجمع المعلومات عن الشبكة والتي تسمح لك بالبحث عن جميع المعلومات المتوفرة حول عناوين IP، اسم المضيف **hostname**، أو الدومين، بما في ذلك البلد، الولاية أو المقاطعة، المدينة، اسم مزود الشبكة، المسؤول، معلومات الاتصال بالدعم الفني. أنه يساعدك أيضا في العثور على مالك الدومين، معلومات الاتصال الخاصة بالمالك، عناوين **IP** الخاصة بالمالك، تاريخ تسجيل الدومين، وما إلى ذلك.

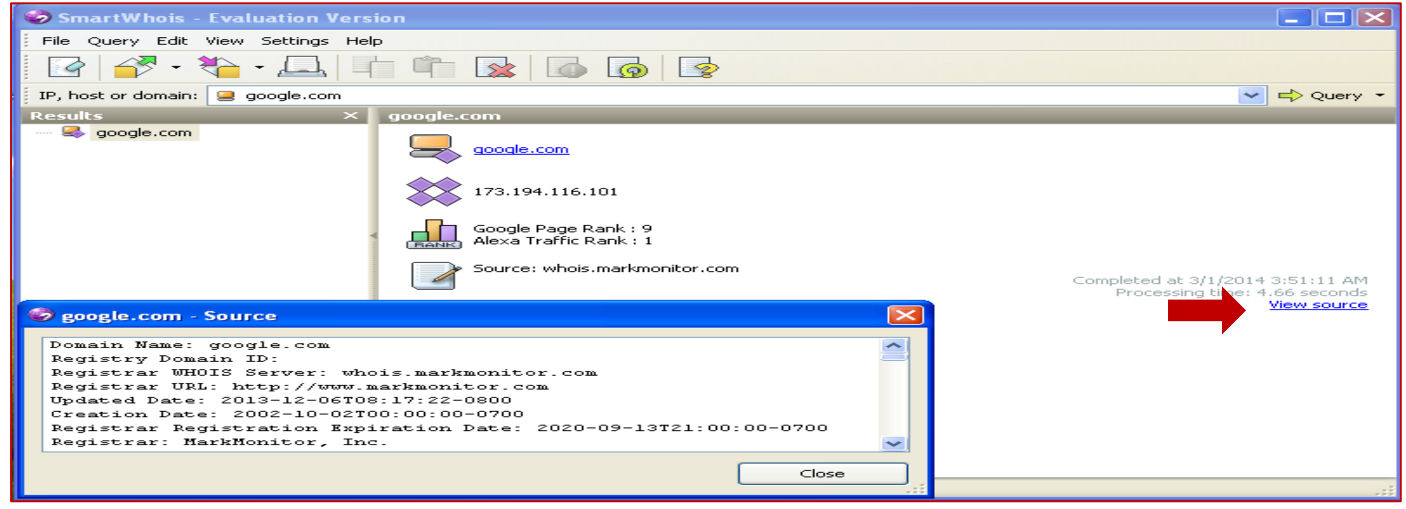
1- نقوم بتثبيت الأداة **SmartWhois** بتباع الـ**wizard** الخاص بعملية التثبيت ثم تشغيله فتظهر الشاشة التالية:



2- في الخانة **IP, host or domain** يكتب اسم الدومين وليكن مثلا google.com ثم نضغط على الزر المقابل له المسمى query ونختار as domain كالاتى:



3- فيعرض لك كل المعلومات عن الدومين باختصار وتلاحظ في الاخر وجود السطر view resource بالضغط عليه يظهر المعلومات بالكامل.



4- يمكنك أيضا استخدامه في الاستعلام عن **hosts** الخاصة بالدومين عن طريق query as IP/hostname وأيضا الاستعلام عن IP عن طريق query as IP وهكذا.

WHOIS LOOKUP TOOLS

مثل الـ **Smartwhois**، هناك العديد من الأدوات المتاحة في السوق لاسترداد معلومات من خدمة **Whois**. سوف نذكر عدد قليل على النحو التالي:

- **Countrywhois**

المصدر **http://www.tamos.com**

Countrywhois هو أداة لتحديد الموقع الجغرافي لعنوان **IP**. **Countrywhois** يمكن استخدامها لتحليل ملفات السجل (**log file**) للخادم، التحقق من رؤوس عناوين البريد الإلكتروني ، تحديد عمليات الاحتيال على بطاقات الائتمان عبر الإنترنت، أو في أية حالة أخرى مثلا اذا كنت في حاجة لتحديد بلد المنشأ بواسطة عنوان **IP** .

ملحوظه: تم استبعاد هذا التطبيق من الشركة المالكة له منذ يناير 2013. لكنه مازال يعمل ويمكن ايجاده عن طريق البحث في شبكة الويب.

- **LanWhoIs**

المصدر **http://lantricks.com**

يوفر **LanWhoIs** المعلومات حول الدومين والعناوين على شبكة الإنترنت. هذا البرنامج يساعدك على تحديد من، أين، ومتى تم تسجيل الدومين أو الموقع الذي يهمك، والمعلومات عن القائمين عليه الآن. هذه الأداة تسمح لك بحفظ نتيجة البحث في شكل ملف أرشيفي لمشاهدته في وقت لاحق. يمكنك طباعة وحفظ نتيجة البحث على هيئة HTML.

- **Batch IP Converter**

المصدر **http://www.networkmost.com**

Batch IP Converter هو أداة للشبكات للعمل مع عناوين IP . فهو يجمع بين **Domain-to-IP Converter**، **Batch Ping**، **Tracert**، **Whois**، **Website Scanner**، و **Connection Monitor** في واجهة واحدة، مثل **IP-to-Country Converter**. فإنه يسمح لك بالبحث عن عنوانين **IP** لواحد أو قائمة من أسماء الدومين والعكس صحيح.

- **CallerIP**

المصدر **http://www.callerippro.com**

CallerIP هو في الأساس اداه لرصد **IP** والمنافذ (**Ports**) التي يعرض الاتصال الواردة والصادرة التي أدخلت على جهاز الكمبيوتر الخاص بك. كما أنه يسمح لك بالبحث عن أصل كل عناوين **IP** على خريطة العالم. توفر ميزة **Whois reporting features** إحصائيات رئيسية مثل الذين يتم تسجيل **IP** إلى عناوين البريد الإلكتروني جنبا إلى جنب مع الاتصال وأرقام الهواتف.

- **WhoIs Lookup Multiple Addresses**

المصدر **http://www.sobolsoft.com**

هذا البرنامج يقدم حلا للمستخدمين الذين يرغبون في البحث عن تفاصيل الملكية لواحد أو أكثر من عناوين IP . يمكن للمستخدمين ببساطة إدخال عناوين **IP** أو تحميلها من ملف. هناك ثلاثة خيارات لمواقع البحث: **whois.domaintools.com**، **whois-search.com** ، و **whois.arin.net**. يمكن للمستخدم تحديد فترة التأخير **delay period** بين عمليات البحث، لتجنب الاغلاق من هذه المواقع. تعرض القائمة الناتجة عناوين **IP** وتفاصيل كل منها. كما يسمح لك لحفظ النتائج إلى ملف نصي.

- **WhoIs Analyzer Pro**

المصدر **http://www.whoisanalyzer.com**

هذه الأداة تسمح لك بالوصول إلى معلومات حول نطاقات الدومين المسجلة في جميع أنحاء العالم، يمكنك عرض اسم مالك الدومين، اسم الدومين، وتفاصيل الاتصال الخاصة بمالك الدومين. كما أنه يساعد في العثور على مكان وجود دومين معين. يمكن أيضا أن يقدم استعلامات متعددة مع هذه الأداة في وقت واحد. هذه الأداة يوفر لك القدرة على طباعة أو حفظ نتيجة الاستعلام على هيئة **html**.

- **Hotwhois**

المصدر **http://www.tialsoft.com**

Hotwhois هو أداة تتبع **IP** التي يمكن أن تكشف عن معلومات قيمة ، مثل البلد ، الدولة، المدينة والعنوان أرقام هاتف الاتصال، و عناوين البريد الإلكتروني وعناوين **IP**. عملية الاستعلام تعطى تقرير عن مجموعة متنوعة من سجلات الإنترنت الإقليمية، وذلك للحصول على

معلومات **Whois** عن عناوين **IP**. باستخدام هذه الأداة يمكنك ان تنشا استفسارات **WHOIS** حتى لو المسجل، يستخدم دومين من النوع **particular domain** أي انه لا يملك خادم لنفسه.

- **ActiveWhois**

المصدر: **http://www.johnru.com**

ActiveWhois هو برنامج قائم على شبكة المعلومات التي تسمح لك بالحصول على معلومات حول أصحاب عناوين IP أو شبكة الدومين. يمكنك أيضا تحديد البلد، والعناوين سواء الشخصية والبريدية للمالك، عناوين IP الخاص بالمستخدمين والدومين.

- **WhoisThisDomain**

المصدر: **http://www.nirsoft.net**

WhoisThisDomain هو تطبيق للبحث عن تسجيلات الدومين والتى تساعدك للحصول على المعلومات حول الدومين المسجلة. حيث انه يكون مرتبط بخادم **whois** بطريقه ما ويحصل منه على سجلات التسجيل للدومين.

هو يدعم كل من **generic domain** و **country code domain**.

- **WHOIS Lookup Online Tools**

بالإضافة الى الأدوات السابقة يوجد بعض الأدوات التي تكون متوفرة على الشبكة والتي تؤدى الى استعلام **whois** كالاتى:

Smartwhois available at **http://smartwhois.com**
Better Whois available at **http://www.betterwhois.com**
Whois Source available at **http://www.whois.sc**
Web Wiz available at **http://www.webwiz.co.uk/domain-tools/whois-lookup.htm**
Network-Tools.com available at **http://network-tools.com**
Whois available at **http://tools.whois.net**
DNSstuff available at **http://www.dnsstuff.com**
Network Solutions Whois available at **http://www.networksolutions.com**
WebToolHub available at **http://www.webtoolhub.com/tn561381-whois-lookup.aspx**
Ultra Tools available at **https://www.ultratools.com/whois/home**

WHOIS في نظام التشغيل لينكس (كالي/باك تراك)

وسيلة بسيطة جدا لكنها فعالة لجمع معلومات إضافية حول هدفنا وهو **whois**. في خدمة **Whois** يتيح لنا الوصول إلى معلومات محددة حول هدفنا بما في ذلك عناوين **IP** أو أسماء المضيفين المسجل في خوادم الاسماء (**DNS**)ومعلومات الاتصال التي عادة ما تحتوي على عنوان ورقم هاتف. بنيت **whois** في نظام التشغيل لينكس أي موجودة افتراضيا. لذلك أبسط طريقة لاستخدام هذه الخدمة عن طريق فتح الترمنال وأدخل الأمر التالي:

$whois©target_domain

```
root@jana:~# whois
Usage: whois [OPTION]... OBJECT...

-l                      one level less specific lookup [RPSL only]
-L                      find all Less specific matches
-m                      find first level more specific matches
-M                      find all More specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match [RPSL only]
-d                      return DNS reverse delegation objects too [RPSL only]
-i ATTR[,ATTR]...       do an inverse lookup for specified ATTRibutes
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned [RPSL only]
-r                      turn off recursive lookups for contact information
-R                      force to show local copy of the domain object even
```

```
root@jana:~# whois syngress.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SYNGRESS.COM
   Registrar: SAFENAMES LTD
   Whois Server: whois.safenames.net
   Referral URL: http://www.safenames.net
   Name Server: NS.ELSEVIER.CO.UK
   Name Server: NS0-S.DNS.PIPEX.NET
   Name Server: NS1-S.DNS.PIPEX.NET
   Status: clientDeleteProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 15-dec-2010
   Creation Date: 10-sep-1997
   Expiration Date: 09-sep-2015

>>> Last update of whois database: Sat, 08 Mar 2014 19:12:21 UTC <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
```

من المهم تسجيل كافة المعلومات وإيلاء اهتمام خاص لخوادم **DNS**. إذا تم سرد خوادم **DNS** بالاسم فقط، سوف نستخدم الأمر **host** لترجمة تلك الأسماء إلى عناوين IP.

يمكن أيضا لـ **Whois**تنفيذ عمليات بحث العكسي. بدلا من إدخال اسم النطاق، أي يمكنك إدخال عنوان IP. سوف تشمل عادة نتيجة **whois** نطاق الشبكة بأكملها الذي ينتمي إلى المنظمة.

```
root@jana:~# whois 173.194.39.18

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#


#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=173.194.39.18?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       173.194.0.0 - 173.194.255.255
CIDR:           173.194.0.0/16
OriginAS:       AS15169
NetName:        GOOGLE
NetHandle:      NET-173-194-0-0-1
Parent:         NET-173-0-0-0-0
NetType:        Direct Allocation
RegDate:        2009-08-17
Updated:        2012-02-24
Ref:            http://whois.arin.net/rest/net/NET-173-194-0-0-1
```

DNS FOOTPRINTING-7 (عملية الاستطلاع عن معلومات DNS)

ملحوظه: تعتبر هذه المرحلة من اهم مراحل الاستطلاع إذا كانت من الممكن ان تغنى عن باقي المراحل.

ننتقل الان الى مرحله أخرى من مراحل عملية الاستطلاع وهي **DNS Footprinting** وفيه هذا الجزء سوف يتم شرح طريق استخراج معلومات **DNS** والأدوات المستخدمة في ذلك.

خوادم **DNS** هي هدف ممتازا للقراصنة ومختبري الاختراق. عادة ما تحتوي على المعلومات التي تعتبر ذات قيمة عالية للمهاجمين. **DNS** هو مكون أساسي في كل من الشبكات المحلية لدينا والإنترنت. من بين أمور أخرى، **DNS** هي المسؤولة عن عملية ترجمة أسماء النطاقات إلى عناوين IP. كبشر، فمن الأسهل بكثير بالنسبة لنا أن نتذكر "**google.com**" بدلا من **74.125.95.105**. مع ذلك، فان آلات يفضلون العكس. يقدم **DNS** كأنه رجل في المنتصف لتنفيذ عملية الترجمة.

كمختبر اختراق، من المهم التركيز على خوادم DNS التي تنتمي إلى هدفنا والسبب بسيط. من أجل DNS يعمل بشكل صحيح، فإنه يجب أن يكون على بينة من كل عناوين IP واسم الدومين المقابل له من كل كمبيوتر على شبكتها. من حيث الاستطلاع، والحصول على حق الوصول الكامل إلى خادم DNS للشركة هو مثل العثور على وعاء من الذهب في نهاية قوس قزح. أو ربما، أكثر دقة، هو مثل العثور على مخططات تسمى blueprint تحتوي على بنية المنظمة الهدف. لكن في هذه الحالة، هذه المخططات Blueprint تحتوي على قائمة كاملة من عناوين IP الداخلية وأسماء المضيف التي تنتمي إلى هدفنا.

نتذكر واحد من العناصر الرئيسية لجمع المعلومات هو جمع عناوين IP التي تنتمي إلى الهدف. بجانب انه وعاء من الذهب، هناك سبب آخر لماذا يركزون على DNS هو انه ممتع جدا في كثير من الحالات هذه الملقمات تميل إلى العمل بمبدأ

"إذا لم يتم كسره، لا تلمس ذلك" [if it isn't broke, don't touch it] يعني انه لا يلمس اعداده إذا لم يتم اختراقه.

إن مسؤولي الشبكة [admin]عديمي الخبرة في كثير من الأحيان يتعاملون مع خوادم DNS بالشك والريبة. في كثير من الأحيان، يختاروا تجاهل هذا المربع تماما لأنهم لا يفهمونه تماما. ونتيجة لذلك، فان ترميم وتحديث أو تغيير إعداد خادم DNS غالبا ما يكون في أولوية منخفضة. هذا إضافة إلى أن معظم خوادم DNS تبدو مستقرة جدا. هؤلاء المدراء يفعلون أكبر خطأ في حياتهم المهنية في وقت مبكر حيث أنهم يفقدوا خوادم DNS الخاصة بهم، بأقل المشاكل صعوبة والتي تسبب لهم فوضى.

يجب ان نتذكر بأن خوادم DNS تحتوي على سلسلة من السجلات [record]التي تحتوي على عنوان IP واسم المضيف لجميع الأجهزة التي على علاقة بالدومين. يتم نشر العديد من خوادم DNS المتعددة (multi DNS) في الشبكة من أجل load balance أو الموازنة. نتيجة لذلك، فان خوادم DNS بحاجة إلى وسيلة لتبادل المعلومات. عملية المشاركة هذه تتم من خلال استخدام نقل المنطقة[zone transferee] . أثناء نقل المنطقة(zone transfer) ، والتي يشار اليها عادة باسم AXFR، حيث يقوم خادم DNS واحد بارسال خوادم DNS الأخرى الى كل المضيفين. هذه العملية تسمح لخوادم DNS المتعددة بالبقاء على وفاق. حتى إذا كنا غير ناجحين في أداء نقل منطقة(zone transfer) ، فلا يزال لدينا بعض الوقت للتحقيق من خوادم DNS التي تقع ضمن نطاق عملنا.

EXTRACTING DNS INFORMATION

DNS Footprinting يسمح لك بالحصول على معلومات حول بيانات DNS Zone. بيانات DNS Zone هذه تشمل أسماء الدومين لل DNSوأسماء أجهزة الكمبيوتر وعناوين ال IP والكثير حول شبكة اتصال معينة. حيث يقوم المهاجم بأداء ال DNS Footprinting على شبكة الاتصال الهدف بغية الحصول على المعلومات حولDNS . يتم استخدام المعلومات التي تم جمعها حول DNS للشبكة الهدف لتحديد المضيفين الرئيسيين (KEY host) في الشبكة وذلك لتنفيذ هجمات الهندسة الاجتماعية في جمع المزيد من المعلومات.

DNS Footprinting يمكن أن يؤدي عن طريق استخدام أدوات مجموعه من الأدوات مثل www.DNSstuff.com والتي بواسطتها يمكن استخراج معلومات ال DNS مثل عناوينIP ، خوادم البريد الملحقة ، DNS Lookup ، Whois Lookup، وهكذا. إذا كنت تريد جمع معلومات حول الشركة مستهدفة، فمن الممكن استخراج نطاق عناوين ال IP المستخدمة (IP range)، المستخدمة في IP Routing. إذا كانت الشبكة الهدف تسمح للمستخدمين الغير مصرح لهم، او الغير معروفين بنقل بياناتDNS zone ، فإنه من السهل عليك الحصول على معلومات حول DNS بمساعدة مجموعه من الأدوات.

بمجرد إرسال استعلام باستخدام أدوات استجواب DNS (DNS Interrogation zone) إلى خادم DNS، فان خادم ال DNS سوف يستجيب لك مع record stricter الذي يحتوي على معلومات حول DNS الهدف. سجلات DNS (DNS record) توفر المعلومات الهامة حول الموقع ونوع الخوادم ومن هذه السجلات (record) كالاتى:

- [A] يشير إلى عنوان IP الخاص المضيف (host's IP address).
- [MX] يشير الى خادم البريد الإلكتروني المرتبط بالدومين (domain's mail server).
- [NS] يشير الى اسم الخادم المضيف المرتبط بالدومين (host's name server).
- [CNMAE] يشير الى الأسماء المستعارة للخوادم المضيفة والمرتبطة بالدومين (aliases to a host).
- [SOA] يشير الى الدومين الرئيسي (authority of domain).
- [SRV] يشير الى الخدمات المسجلة (service record).
- [PTR] يشير الى عناوين IP الخاص بالدومين وتستخدم في الاستعلام العكسي لل DNS (IP address to a host name).
- [RP] تشير الى الأشخاص المسئولين (responsible person).
- [HINFO] تشير الى معلومات عن الأجهزة المضيفة المرتبطة بالدومين الرئيسي مثل معلومات عن نظام التشغيل و CPU المستخدم وهكذا (HOST information record).

الأدوات المستخدمة في ارسال طلب استعلام عن سجلات DNS RECORD كالاتى:

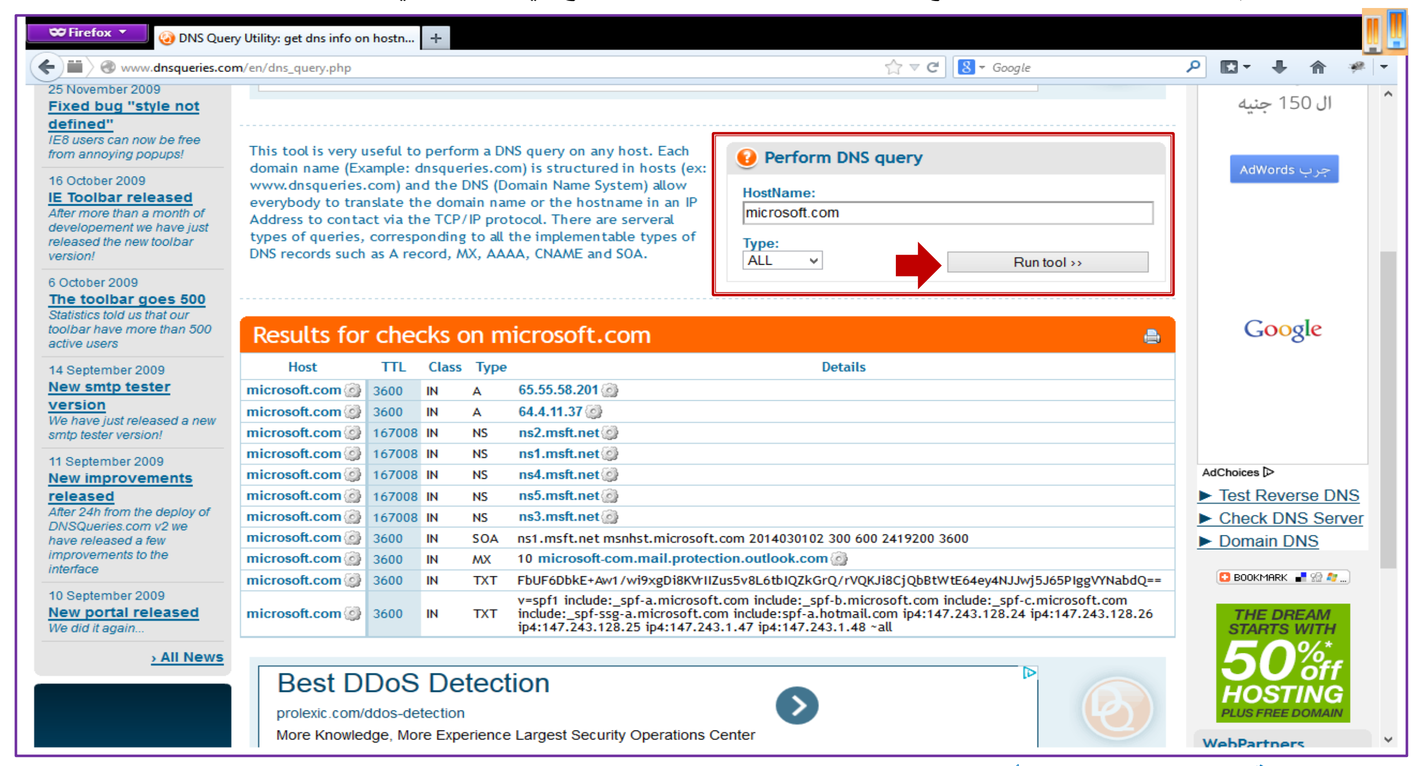
http://www.dnsstuff.com
http://network-tools.com
Ping – nslookup - dig

- استخراج معلومات DNS (Extracting DNS information) باستخدام http://www.dnsqueries.com

يمكنك أداء عملية الاستعلام عن DNS عن طريق استخدام موقع الويب http://www.dnsqueries.com والتي تعتبر أداة تسمح لك بتنفيذ أي استعلام عن DNS على أي المضيف. كل اسم دومين على سبيل مثال (dnsqueries.com) عباره عن تركيب مع المضيفين (hosts) على سبيل المثال (www.dnsqueries.com) و((DNS (Domain name system) يسمح لأي شخص بترجمة اسم الدومين أو اسم المضيف الى عنوان IP ليتم الاتصال باستخدام البروتوكول TCP/IP .

هناك عدة أنواع من الاستعلامات، والتي تعبر عن نوع سجلات DNS مثل MX، AAAA ، CNAME وSOA.

الآن دعونا نرى كيف أداة عملية الاستطلاع عن DNS باستخدام تلك الأداة. وذلك عن طريق الذهاب إلى متصفح الويب وكتابة http://www.dnsqueries.com ثم الضغط على Enter. سوف يتم عرض صفحة الويب الخاصة بهذا الموقع. نقوم بإدخال اسم الدومين الذي تريد الاستعلام في الحقل Perform DNS query (هنا أننا ندخل موقع Microsoft.com) وانقر فوق الزر أداة التشغيل run tool؛ سيتم عرض معلومات DNS لموقع Microsoft.com كما هو موضح في الشكل التالي.



- عملية الاستطلاع باستخدام الأداة Ping

Ping: هو اختصار لـ packet Internet Groper. هو أداة معروفة لأغلب مهندسي وخبراء تقنية المعلومات. يعتبر أمر من الأوامر المستخدمة في سطر الاوامر (مثال LINUX, MSDOS, UNIX)، وذلك لغرض الفحص والتحقق من الاتصال بمستوى IP مع كمبيوتر آخر أو موجه Router أو طابعة أو أي جهاز آخر يستخدم بروتوكول TCP/IP. يرسل الأمر ping مجموعة من حزم من البيانات إلى جهاز آخر مشترك في نفس الشبكة ويطلب منه الرد بإشارات معينة على هذه الحزم ثم يعرض النتائج بأكملها على الشاشة.

لذلك فان الامر ping يستخدم في الاتي:

1. التعرف على حالة الشبكة وحالة المستضيف (موقع ما أو صفحة).
2. تتبع وعزل الأعطال في القطع والبرامج.
3. لاختبار وإدارة الشبكة.
4. يمكن استخدام الأمر ping لعمل فحص ذاتي للحاسب(loopback) .

لكن يوجد استخدام اخر لهذه الأداة من قبل القراصنة والتي من شأنها أن تسمح لك بجمع المعلومات المهمة مثل عنوان IP، الحد الأقصى لحجم حزم (frame size) وبعض المعلومات الأخرى. يستخدم أيضا من قبل penetration tester من اجل التأكد من الوصول لجهاز الكمبيوتر الخاص بهم الى الشبكة.



كيف يعمل الامر ping؟

يعمل الامر **ping** من خلال إرسال حزمه من البيانات باستخدام البروتوكول (Internet Control Message Packet) ICMP إلى الحاسب الأخر (echo request packet) ومن ثم الانتظار للحصول على رد لتلك الحزمة من البيانات (ICMP response). ومن خلال عملية الانتظار للحصول على رد فان الامر ping يعمل على قياس الوقت المستخدم من ارسال الحزمة حتى الحصول على الرد وهذا يعرف بـ round-trip timeويقوم أيضا بتسجيل أي حزمه تم فقدانها.

في نظام التشغيل ويندوز:

مثال على الامر **ping** نقوم بكتابة الامر التالي في **command prompt (cmd)** في الويندوز.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.certifiedhacker.com

Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.54.101: bytes=32 time=680ms TTL=112
Reply from 202.75.54.101: bytes=32 time=396ms TTL=112
Reply from 202.75.54.101: bytes=32 time=394ms TTL=112
Reply from 202.75.54.101: bytes=32 time=450ms TTL=112

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 394ms, Maximum = 680ms, Average = 480ms

C:\WINDOWS\system32>
```

>ping©www.certifiedhacker.com

ستلاحظ المعلومات التالية نتيجة استخدام الامر ping:

انه تم ارسال 4 حزم من المعلومات **Packets** ولم يفقد منها شيء. حيث الخانة **sent=4** و **received =4** و **lost =0** والتي تعنى انه لم يفقد أي حزمه. كما سترى أيضا معلومة الزمن الذي أخذته كل حزمة في الذهاب والعودة بالميلي ثانية. كما يوضح أيضا الحجم الأساسي للحزمة الواحدة وهي 32 بايت

نلاحظ ايضا اننا حصلنا على بعض المعلومات الأخرى مثل عنوان **IP** المقابل لـ **www.certifiedhacker.com** وهو 202.75.53.101 ويمكن أيضا الحصول على معلومات عن الحزمة **packet** التي تم ارسالها مثل عدد الحزم التي تم ارسالها وأيضا التي تم استقبالها، عدد الحزم التي فقدت في الطريق وأيضا **approximate round trip times**.

الشكل العام لأمر ping

Ping [-t] [-a] [-n] [-l] [-f] [-i] [-v] [-r] [-s] [-w] [-j] targetname

هناك بعض المعايير المستخدمة مع الامر ping:

هنالك بعض المعايير الاختيارية والتي توضع مع الأمر **ping**وهي:

(**-t**) والتي تخبر الامر **ping** بان يستمر بالإرسال للعنوان المطلوب حتى يتوقف عن الإجابة وإذا أردنا مقاطعة الإحصائيات وعرضها نضغط, **CTRL+Break** ولمقاطعة **ping**وإنهائه نستخدم**CTRL+C** .

(**-a**) لعرض الرقم التعريفي للعنوان المحدد.

يمكن أيضا استخدامه لمعرفة أكبر حجم للحزم (max frame size) من الممكن ارساله بواسطة الامر **ping** كالاتى:

```
C:\WINDOWS\system32>ping www.certifiedhacker.com -f -l 1500

Pinging www.certifiedhacker.com [202.75.54.101] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>
```

نلاحظ انه اعطى هذه الرسالة [**Packet needs to be fragmented but DF set.**] والتي تعنى انه يريد منك تجزئة حجم الرسالة وتصغيرها حيث استخدمنا (**–l**) والتي يمكن تحديد حجم الرسالة عن طريقه حيث الحجم الافتراضي هو 32 بايت واستخدمنا أيضا معه الصيغة (**–f**) حتى لا يقوم بتجزئة الرسالة وارسالها مرة واحده. نقوم الان بتصغير الحجم تدرجيا وليكن مثلا 1300 كالاتى:

```
C:\WINDOWS\system32>ping www.certifiedhacker.com -f -l 1300

Pinging www.certifiedhacker.com [202.75.54.101] with 1300 bytes of data:
Reply from 202.75.54.101: bytes=1300 time=509ms TTL=112
Reply from 202.75.54.101: bytes=1300 time=510ms TTL=112
Reply from 202.75.54.101: bytes=1300 time=509ms TTL=112
Reply from 202.75.54.101: bytes=1300 time=507ms TTL=112

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 507ms, Maximum = 510ms, Average = 508ms

C:\WINDOWS\system32>
```

نجد انه قام بارسال الرسالة نستنتج من ذلك ان اقصى حجم للرسال يمكن ارساله بواسطة **Ping** يندرج بين 1500 و1300
نحاول تجربة الأرقام من 1300 و1500 فلنجرب مثلا 1473 كالاتي:

```
C:\WINDOWS\system32>ping www.certifiedhacker.com -f -l 1473

Pinging www.certifiedhacker.com [202.75.54.101] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>
```

نجد انه لم ينجح في الارسال فلنجرب 1472 كالاتي:

```
C:\>ping www.certifiedhacker.com -f -l 1472

Pinging www.certifiedhacker.com [202.75.54.101] with 1472 bytes of data:
Reply from 202.75.54.101: bytes=1472 time=359ms TTL=114
Reply from 202.75.54.101: bytes=1472 time=320ms TTL=114
Reply from 202.75.54.101: bytes=1472 time=282ms TTL=114
Reply from 202.75.54.101: bytes=1472 time=317ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 282ms, Maximum = 359ms, Average = 319ms

C:\>
```

نجد هنا انه نجح في الارسال إذا أكبر حجم ممكن للرسالة التي يرسلها الامر ping لهذا الموقع هو 1472.

نجد ان الصيغة المتحكمة في حجم الرسالة/الحزمة (frame size) هنا (-l).

جميع الحزم (**FRAME**) تملك صلاحية **TTL** (**Time to live**) والتي عند وصولها الى الرقم صفر فان الموجه **router** يقوم باستبعاده حيث يستخدم هذه التقنية في منع فقد الحزم (**loss of packet**).

يمكن أيضا استخدام الصيغة (**-i**) والتي تحدد المدة الزمنية لكل حزمة ومقاسة بالميلي ثانية او بمعنى اصح تستخدم في وضع قيمة **TTL** لكل حزمه. يمكن أيضا استخدام الصيغة (**-n**) والتي تتحكم في عدد الحزم المرسلة حيث العدد الافتراضي هو 4.

في نظام التشغيل جنو/لينكس

الصيغة العامة للأمر **ping** في لينكس كالاتي:

ping [-c count] [-i interval] [-l preload] [-p pattern] [-s packetsize] [-t ttl] [-I interface] [-T timestamp option] [-W timeout] destination

```
root@jana:~# ping www.google.com
PING www.google.com (173.194.113.144) 56(84) bytes of data.
64 bytes from ham02s11-in-f16.1e100.net (173.194.113.144): icmp_req=1 ttl=45 tim
e=868 ms
64 bytes from ham02s11-in-f16.1e100.net (173.194.113.144): icmp_req=2 ttl=45 tim
e=1184 ms
64 bytes from ham02s11-in-f16.1e100.net (173.194.113.144): icmp_req=3 ttl=45 tim
e=1290 ms
64 bytes from ham02s11-in-f16.1e100.net (173.194.113.144): icmp_req=4 ttl=45 tim
e=1503 ms
^C64 bytes from ham02s11-in-f16.1e100.net (173.194.113.144): icmp_req=5 ttl=45 t
ime=1101 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 6672ms
rtt min/avg/max/mdev = 868.603/1189.831/1503.831/209.613 ms, pipe 2
root@jana:~#
```

حيث نلاحظ اننا قمنا بكتبة الامر **ping** متبوعا باسم الـ **host**. فنجد انه تم ارسال الحزم ولكن نجد انه لا يتوقف حتى نقوم بالضغط على **Ctrl+C** ونجد انه يعطى رسالة لتوضيح **ttl** والوقت المستغرق في ارسال الحزمة نجد انه هو الاخر يأتي معه العديد من الخيارات كالاتى:

Table 5-1. Command Line Switches for the ping Command

Switch	Effect
-c *count*	Send only *count* echo requests before exiting.
-i *interval*	Pause *interval* seconds between echo requests.
-w *timeout*	Exit after *timeout* seconds have passed, even if all echo replies have not been received.
-b	Allow the specified address to be a network or broadcast address, effectively pinging every host on the specified network. (Only available to the root user.)
-f	Ping flooding. Send echo requests as quickly as possible. For every request sent, print a ".". For every reply received, print a backspace. A resulting progression of periods across the screen implies packets are being dropped by the network. (Only available to the root user).

المشكلة مع الأمر **ping** هو أنه يسمح لك باستخدام **ICMP** للتحقق من مضيف واحد [**host**]في وقت واحد. الأمر **fping** يسمح لك بتتبع العديد من المضيفين [**multiple host**] باستخدام امر واحد. سوف تتيح لك أيضا قراءة ملف به أسماء المضيفين المتعددة أو عناوين IP وإرسالها باستخدام حزمة**ICMP echo requests**. لاستخدام الأمر **fping** لتشغيل **ICMP swap** على الشبكة، عن طريق اتباع التالي:

```
fping-asg network/host bits
fping -asg 10.0.1.0/24
```

ملحوظه: التعبير g يستخدم إذا كنت تستخدم عنوان IP.

```
root@jana:~# fping -as www.google.com
www.google.com

        1 targets
        1 alive
        0 unreachable
        0 unknown addresses

        0 timeouts (waiting for response)
        1 ICMP Echos sent
        1 ICMP Echo Replies received
        0 other ICMP received

 135 ms (min round trip time)
 135 ms (avg round trip time)
 135 ms (max round trip time)
        0.136 sec (elapsed real time)

root@jana:~#
```

- **الأداة nslookup**

NSLOOKUP هو الأداة التي يمكن استخدامها للاستعلام من ملقمات DNS وربما الحصول على سجلات حول مختلف المضيفين التي هي على علم بها. بنيت **NSLOOKUP** في العديد من إصدارات لينكس بما في ذلك كالي وحتى يتوفر لنظام التشغيل **Windows**. **NSLOOKUP** يعمل بطريقة مماثلة جدا بين مختلف أنظمة التشغيل، ولكن يجب مراجعة دائما خصوصيات لنظام التشغيل الخاصة بك. يمكن استخدام الأداة **nslookup** من قبل القراصنة للحصول على عنوان **IP** لدومين معين والذي يتيح له في إيجاد عنوان **IP** الخاص بالشخص الذي يأمل في مهاجمته. على الرغم من أنه من الصعب تقيد المستخدمين الأخرين للاستعلام مع خادم **DNS** باستخدام الأمر nslookupلأن هذا البرنامج يعتبر محاكاة لعملية قيام البرامج الأخرى من ترجمة الأسماء من خلال طلبات لخادم **DNS**، ووظيفة مختبر الاختراق [**penetration tester**] هو أن يكون قادر على منع مثل هذه الهجمات من خلال الذهاب الى **zone proprieties'**. في **zone transfer tab**. تحديد خيار لعدم السماح بـ**zone transfer**. هذا لمنع المهاجمين من استخدام الأمر **nslookup** للحصول على قائمة لسجلات المنطقة (zone's record) الخاص بك. **NSLOOKUP** يمكن أن يوفر لك ثروة من المعلومات التشخيصية لخادم **DNS**.

NSLOOKUP هو الأداة التي يمكن تشغيلها في الوضع التفاعلي [**interactive mode**]. هذا يعني ببساطة أننا سوف نستدعى البرنامج أولا ثم نطعمه بمفاتيح معينة حتى نجعله يعمل بشكل صحيح. نبدأ باستخدام **NSLOOKUP** من خلال فتح الترمنال (**terminal**)في اللينكس او **command prompt** في الويندوز والدخول الى الامر عن طريق كتابة **nslookup**:

Command prompt in windows

```
C:\WINDOWS\system32>nslookup
Default Server:  UnKnown
Address:  192.168.16.1

> help
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,
SOA,SRV)
    querytype=X         - same as type
    class=X             - set query class (ex. IN (Internet), ANY)
    [no]msxfr           - use MS fast zone transfer
    ixfrver=X           - current version to use in IXFR transfer request
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -d          -  list all records
    -t TYPE     -  list records of the given RFC record type (ex. A,CNAME,MX,NS,
PTR etc.)
view FILE           - sort an 'ls' output file and view it with pg
exit            - exit the program

>
```

Terminal in Linux

```
root@jana:~# nslookup
> 
```

بإصدار الأمر "**nslookup**"، نكون قد بدانا **nslookup** من نظام التشغيل. بعد كتابة "**nslookup**" ثم **Enter**، سوف يتم استبدال المحث الافتراضي سواء في الويندوز او لينكس الى الرمز[>]. ولكن قبل هذا فانه سوف يعرض بيانات الملقم الذي نستخدمه في عمليات الفحص اليومية عبر الانترنت واقصد هنا الملقم الخاص بمقدمي خدمة الانترنت (**ISP**). يمكنك أيضا معرفة هذا عن طريق كتابة الكلمة **server** بدون أي إضافات. عند هذه النقطة، يمكنك إدخال المعلومات الإضافية التي يحتاجها **NSLOOKUP** لكي يعمل. نبدأ بتغذية الأمر **NSLOOKUP** عن طريق إدخال الكلمة "**server**" الكلمة وعنوان IP لملقم DNS التي تريد الاستعلام عنه. مثال كالتالي:

>server©8.8.8.8

ملحوظه: للاستعلام عن اسم ملقم آخر مباشرة، نستخدم الأمر **server** أو الأمر **lserver** للتبديل إلى الملقم الاسم هذا. يستخدم الأمر **lserver** الملقم المحلي للحصول على عنوان الملقم للتبديل إليه بينما يستخدم الأمر **server** الملقم الافتراضي الحالي للحصول على العنوان.

```
> server
Server:  UnKnown
Address:  192.168.16.1

*** UnKnown can't find server: Non-existent domain
> server 8.8.8.8
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> server
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

*** google-public-dns-a.google.com can't find server: Non-existent domain
> _
```

NSLOOKUP سوف يقبل الامر ببساطة ويقدم لكل سطر آخر مع العلامة ">". نحن نريد تحديد نوع السجل الذي نبحث عنه. أثناء عملية الاستطلاع، هناك أنواع عديدة من السجلات التي ربما كنت مهتما بها. للحصول على قائمة كاملة من الأنواع المختلفة لسجل **DNS** ووصفهم، يمكنك استخدام المهارات المكتسبة حديثا من خلال بحث جوجل الخاص بك. إذا كنت تبحث عن معلومات عامة، يجب تعيين **type** إلى **any** باستخدام الكلمة الأساسية "**any**" كالآتى:

>set type=any

نتأكد من عدم وجود تباعد/مسافة أو ستحصل على رسالة خطأ. نكتب اسم الدومين الذي تريد ان تبحث عنه. إذا كنت تبحث عن معلومات محددة من ملقم **DNS** مثل عنوان **IP** لملقم البريد الذي يتعامل مع البريد الإلكتروني للمنظمة الهدف، نستخدم التسجيل[**set type=mx**] .

ثم نختم استجواب DNS الأولي لدينا مع NSLOOKUPعن طريق إدخال الدومين الهدف بعد العلامة [>].

```
> set type=any
> syngress.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
syngress.com    nameserver = ns0-s.dns.pipex.net
syngress.com    nameserver = ns1-s.dns.pipex.net
syngress.com    nameserver = ns.elsevier.co.uk
syngress.com
        primary name server = ns.elsevier.co.uk
        responsible mail addr = hostmaster.elsvier.co.uk
        serial  = 2014031103
        refresh = 3600 (1 hour)
        retry   = 900 (15 mins)
        expire  = 2419200 (28 days)
        default TTL = 900 (15 mins)
syngress.com    internet address = 50.87.186.171
syngress.com    MX preference = 10, mail exchanger = syngress.com.inbound10.mxlo
gic.net
syngress.com    MX preference = 10, mail exchanger = syngress.com.inbound10.mxlo
gicmx.net

ns1-s.dns.pipex.net     internet address = 158.43.193.83
ns.elsevier.co.uk       internet address = 193.131.222.35
ns0-s.dns.pipex.net     internet address = 158.43.129.83
>
```

نفترض أنك تريد أن تعرف ما هو خادم البريد المستخدمة للتعامل مع البريد الإلكتروني للsyngress.com. في المثال السابق، توصلنا إلى أن واحدة من خوادم اسماء Syngress كان "ns.elsevier.co.uk". هنا مرة أخرى، يمكننا استخدام نوع السجل كالآتي:

```
> syngress.com
Server:  [8.8.8.8]
Address:  8.8.8.8

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
syngress.com    MX preference = 10, mail exchanger = syngress.com.inbound10.mxlo
gicmx.net
syngress.com    MX preference = 10, mail exchanger = syngress.com.inbound10.mxlo
gic.net
>
```

ملحوظه: إذا اعطى لك timeout فاستخدمه مرة أخرى حتى يستجيب DNS الى طلبك.

نفس ما سبق في جنو لينكس كالاتى:

```
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> server
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=any
> syngress.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
syngress.com
        origin = ns.elsevier.co.uk
        mail addr = hostmaster.elsvier.co.uk
        serial = 2014031103
        refresh = 3600
        retry = 900
        expire = 2419200
        minimum = 900
syngress.com    nameserver = ns1-s.dns.pipex.net.
syngress.com    nameserver = ns.elsevier.co.uk.
syngress.com    nameserver = ns0-s.dns.pipex.net.

Authoritative answers can be found from:
ns.elsevier.co.uk       internet address = 193.131.222.35
>
```

نلاحظ هذه الرسالة **autherative answer can be found from** ثم اعطى اسم خادم الأسماء الخاص به. هذا يخبرك انه لكي تحصل على اجابه اكيده يمكنك سؤال هذا الخادم. لاحظنا سابقا عند الاستعلام عن الدومين **Syngress** نجد انه يحتوي على ثلاث خوادم/ملقمات **DNS** يتعامل معها ونجد ان الملقم الرئيسي لهم والذي طلب منك سؤاله حتى تحصل على اجابه اكيده هو [**ns.elsevier.co.uk**]. نذهب الى هذا الخادم/الملقم باستخدام التعبير [**server**] ثم اسم ملقم/خادم الاسماء DNS. هذا يعنى كما قلنا سابقا اننا سوف نستخدم هذا الخادم/الملقم في السؤال عن الدومين الذي نريده. نفترض هنا أيضا اننا نريد تحديد السجل [**record**]مثلا **mx** لمعرفة ملقمات/خوادم البريد الإلكتروني كالاتى:

```
> server 193.131.222.35
Default server: 193.131.222.35
Address: 193.131.222.35#53
> set type=mx
> syngress.com
Server:         193.131.222.35
Address:        193.131.222.35#53

syngress.com    mail exchanger = 10 syngress.com.inbound10.mxlogicmx.net.
syngress.com    mail exchanger = 10 syngress.com.inbound10.mxlogic.net.
> 
```

تلخيص ذلك: ان عملية **nslookup** تتم في الوضع **interactive mode** او في الوضع **non-interactive mode**. لتشغيل **nslookup** في الوضع **interactive mode** ويتم ذلك عن طريق كتابة الامر **nslookup** بدون أي صيغ اضافيه او استخدام الصيغة (-) ثم يليه اسم المضيف **hostname** او عنوان **ip** في الـ **command prompt**. الذي يؤدى الى الدخول الى الامر وظهور العلامة(**>**).
اما لتشغيله في الوضع **non-interactive mode** فيتم ذلك عن طريق كتابة الامر **nslookup** ثم يتبعه أي من الصيغ التالية سواء اسم المضيف **hostname** او عنوان **ip** (**IP address**).
عند استخدام الأداة **nslookup** فإنك سوف تستقبل **authoritative answer** او **non-authoritative answer**. تكون الإجابة غير موثقه (**non-authoritative answer**) وذلك لان **nslookup** افتراضيا يسال خادم الأسماء **nameserver** من اجل ترجمة الاستعلام الخاص به. وخادم الأسماء الخاص بك (**nameserver**) يكون غير موثق **not authority** لاسم الذي تسال عنه. يمكنك أيضا الحصول على اجابه موثقه (**autheratívite answer**) عن طريق ارسال الطب الى خوادم أسماء موثقه (**autherative nameserver**) عن أسماء الدومين التي تريد الاستعلام عنه.

ما الاستخدام الاخر الهام لهذه الأداة؟

يمكن استخدام الأداة **Nslookup** لنقل منطقة كاملة [**zone transfer**] باستخدام الأمر **ls**. يكون هذا الأمر مفيدًا لمعرفة كافة المضيفين داخل الدومين البعيد (بمعنى اصح معرفة كل السجلات (**record**)الداخلية والخارجية). يكون بناء الجملة للأمر **ls** كالتالي:

>ls [- a | d | t type] domain [> filename]

يؤدي استخدام الأمر **ls** بدون وسائط إلى إرجاع قائمة بكافة بيانات العناوين وأسماء الملقمات. يؤدي التعبير[**-a**] إلى إرجاع الاسم المستعار والأسماء المتعارف عليها [**canonical names and aliases**]، بينما يؤدي التعبير [**-d**] إلى إرجاع كافة البيانات والتعبير [**-t**] إلى التصفية حسب النوع.
يمكن حظر عمليات نقل المنطقة (**zone transfer**) في ملقم **DNS** بحيث تقوم العناوين أو الشبكات الموثوقة فقط بإجراء هذه الوظيفة. يظهر الخطأ التالي في حالة تعيين أمان المنطقة (منع عملية نقل المنطقة):

*****Can't list domain example.com.: Query refused**

- **الأداة dig**

Dig أداة أخرى عظيمة لاستخراج المعلومات من**DNS** . تعمل مع نظام التشغيل لينكس فقط للعمل مع الامر **dig**، فنحن ببساطة نفتح الترمنال وندخل الأمر التالي:

```
dig @target_ip
```

بطبيعة الحال، سوف يتم استبدال "**target_ip**" مع عنوان **IP** الفعلي الذي تستهدفه. من بين أمور أخرى، **dig** يجعل من السهل جدا محاولة نقل المنطقة لذلك فهو تطوير لـ **nslookup** وأسهل منه في عملية نقل المنطقة (**zone transfer**). تجدر الإشارة إلى أن نقل المنطقة يستخدم لسحب سجلات متعددة من خادم **DNS**. في بعض الحالات، يمكن أن يؤدي نقل منطقة في إرسال ملقم **DNS** المستهدفة

كافة السجلات التي يحتوي عليها. هذا هو قيمة خاصة إذا كان الهدف الخاص بك لا يميز بين عناوين **IP** الداخلية والخارجية عند إجراء نقل المنطقة(**zone transfer**) .

يمكننا محاولة نقل المنطقة مع dig باستخدام التعبير[**-t©AXFR**]. إذا أردنا محاولة نقل المنطقة من الدومين ذات العنوان **IP** 192.168.1.23 الى دومين وهمى "example.com"نكتب الأمر التالي:

```
dig©@192.168.1.23©example.com©-t©AXFR
```

إذا سمح بعملية نقل المنطقة ولم تمنع، فإنك سوف تملك قائمة بأسماء المضيفين وعناوين **IP** من ملقم **DNS** المستهدف.

- **بعض الأدوات الأخرى المستخدمة في عملية الاستطلاع عن DNS عن دومين معين كالاتى:**

DIG available at **http://www.kloth.net**
myDNSTools available at **http://www.mydnstools.info**
Professional Toolset available at **http://www.dnsstuff.com**
DNS Records available at **http://network-tools.com**
DNSData View available at **http://www.nirsoft.net**
DNSWatch available at **http://www.dnswatch.info**
DomainTools Pro available at **http://www.domaintools.com**
DNS Lookup Tool available at **http://www.webwiz.co.uk**
DNS Query Utility available at **http://www.webmaster-toolkit.com**

الأدوات المستخدمة في عملية الاستطلاع عن DNS في نظام التشغيل كالي/باك تراك فقط

في هذا الجزء، سوف نؤدي بعض الحيل باستخدام خدمة التعداد "**enumeration service**". خدمة التعداد هى العملية التي تسمح لنا بجمع المعلومات من الشبكة. سوف نقوم بدراسة تقنيات تعداد **DNS** [**DNS enumeration**]. تعداد **DNS** هي عملية تحديد كافة الخوادم لل **DNS** وإدخالات **DNS** للمنظمة الهدف. تعداد **DNS** سوف يسمح لنا بجمع المعلومات الهامة عن المنظمة مثل أسماء المستخدمين وأسماء أجهزة الكمبيوتر، عناوين **IP**، وهكذا. **كيف تفعل هذا؟**

- **الأداة DNSwalk**

هذه الأداة هي **DNS database debugger**. ينفذ عمليات نقل المنطقة (**zone transfer**) من الدومين المحدد، ويتحقق من قاعدة البيانات بطرق عديدة لفحص التوافق الداخلي، وكذلك التصحيح وفقا للتصريح الممنوح من قبل الملقم **DNS**. هذه الأداة مبرمجة بلغة بيرل. **اسم الدومين المحدد في سطر الأوامر يجب أن تنتهي '.'.**

طريقة استخدامها:

تستخدم مع اسم الدومين هكذا [**dnswalk©podunk.edu.**]. أو اسم الدومين العكسي، مثل [**dnswalk©3.2.1.in-addr.arpa.**].

- **الأداة dnsenum:**

هذه الأداة اقوى من **dnswalk** ومبرمجه هي الأخرى بلغة بيرل. تعمل هذه الأداة عن طريق كتابة الامر التالي في الترمنال

```
$dnsenum©--enum©www.google.com
```

```
root@jana:~# dnsenum --enum www.google.com
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries disabled.

-----   www.google.com   -----


Host's addresses:
__________________

www.google.com                           87       IN     A          173.194.113.144
www.google.com                           87       IN     A          173.194.113.145
www.google.com                           87       IN     A          173.194.113.147
www.google.com                           87       IN     A          173.194.113.148
www.google.com                           87       IN     A          173.194.113.146


Name Servers:
______________

 www.google.com NS record query failed: NOERROR
root@jana:~#
```

ما نوع المعلومات التي يمكن جمعها بواسطة dnsenum؟

1- الحصول على عنوان المضيف (hosts address) (السجل A) / الحصول على خوادم الأسماء DNS / الحصول على سجل mx .
2- تنفيذ استعلامات AXFR على خوادم الأسماء (DNS) والحصول على إصدارات BIND .
3- الحصول على أسماء النطاقات الفرعية الاضافية (subdomain)والاسماء الإضافية (extra name) عن طريق استخدام استعلاء جوجل المتقدم (google scraping).
4- استخدام تقنية Brute force في تخمين أسماء الناطاقات الإضافية (subdomain name) وذلك بواسطة ملف txt يحتوي على (95 sub domain name) ليجربها في محاولته لمعرفة أسماء النطاقات الفرعية الحقيقية (subdomain name).
5- يحسب نطاقات الشبكة من الفئة C وتنفيذ استعلامات whois عليها.
6- تنفيذ عمليات البحث العكسي (reverse lookup).
7- كتابة الناتج إلى ملف txt.

هناك بعض الخيارات الإضافية التي يمكن تشغيلها باستخدام Dnsenum وأنها تشمل ما يلي:

يسمح لك بتعيين عدد العمليات التي سوف يتم تشغيلها في وقت واحد	--threads [number]
يسمح لك بتمكين عمليات البحث العكسي [recursive lookup]	-r
يسمح لك بتعيين تأخير الوقت بالثواني بين طلبات whois	-d
يسمح لك لتحديد مكان إخراج الناتج	-o
يسمح لك بتمكين استعلامات whois على نطاق الشبكة من النوع سي	-w

--enum = [--threads 5 –s 20 –w]

يمكنك الاطلاع على باقي التعبيرات باستخدام man.

▪ الأداة dnsmap

هي أيضا تأتى مماثله للأداتين السابقتين (dnswalk , dnsenum) من ناحية إيجاد أسماء النطاقات الفرعية (subdomain name). هذه الأداة يأتي معها wordlist من أجل عملية التخمين (brute forcing). هذه الأداة يمكنها تخزين نتائجها في ملف، ويمكن استخدامها بدون صلاحيات المستخدم الجذري (root privilege).
لاستخدام هذا الامر نكتب في الترمنال dnsmap كالاتى:

```
root@jana:~# dnsmap
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

usage: dnsmap <target-domain> [options]
options:
-w <wordlist-file>
-r <regular-results-file>
-c <csv-results-file>
-d <delay-millisecs>
-i <ips-to-ignore> (useful if you're obtaining false positives)

e.g.:
dnsmap target-domain.foo
dnsmap target-domain.foo -w yourwordlist.txt -r /tmp/domainbf_results.txt
dnsmap target-fomain.foo -r /tmp/ -d 3000
dnsmap target-fomain.foo -r ./domainbf_results.txt

root@jana:~#
```

عند كتابة هذا الامر بدون أي تعبيرات أخرى فانه يعطيك قائمه بجميع التعبيرات التي من الممكنة ان تستخدم معه.
[-w] يكتب بعدها مسار الملف wordlist الذى سوف يستخدم في brute forcing.
[-r] هذه تعنى regular-results-file تستخدم في تنظيم ناتج الامر في ملف الناتج.
[-c] هي اختصار ل CSV وهى نوع الملف الذى سوف تخزن فيه النتائج بطريقه منتظمة.
[-d] هي اختصار لكلمة delay وتعنى التأخير وذلك بالملي ثانيه.
[-i] هو اختصار ل IP وتعنى هنا IP الذى تريد تجاوزه في عملية الفحص (IP's To Ignore).
ثم بعد ذلك امثله لطريقة استخدام هد الامر. هذه الأداة تأخذ بعض من الوقت لكي تعطى نتيجة نهائية.

▪ الأداة dnsrecon

هي أيضا اداه تشابه الأدوات السابقة الذكر وتقوم تقريبا بنفس المهام وتستخدم brute force لمعرفة النطاقات الفرعية (subdomain). تعمل هده الأداة في شكل استعلام (query) وذلك على NS وSOA وسجلات MX. هذه الأداة تم تطويرها من قبل كارلوس بيريز باستخدام لغة البايثون.

في الوقت التي تم الكتابة فيه عن هذه الأداة، فإنها تدعم الاتي:

1- معرفة أسماء النطاقات الإضافية (subdomain) وأسماء المضيفين (hostname) باستخدام تقنية brute force.
2- تدعيم البحث عن السجلات الأساسية في ملقم DNS (A,NS,SOA,MX).
3- التوسع في عمليات البحث الى TLD وذلك للدومين الهدف.
4- يدعم نقل المنطقة (zone transfer) لجميع سجلات NS.
5- يدعم البحث العكسي(Reverse Lookup) .
6- يدعم سجلات SRV.

يبدا عمل هذه الأداة عن طريق كتابة الامر dnsrecon.py مع مجموعه من التعبيرات لتحديد طريقة عملها في الترمنال.

نجد ان هذه الأداة تأتى بمجموعه من التعبيرات/الخيرات التي تتيح لك الكثير من المميزات كالاتى:

1- استخدام هذه الأداة للحصول على السجلات التقليدية من ملقم DNS للدومين الهدف وذلك عن طريق استخدام التعبير [-d] والذي يوضع بعده اسم الدومين المستهدف. نستخدم معه أيضا الخيار [-t] وذلك لتحديد نوع عملية الاستطلاع الذي تريده والذي يأتي معه العديد من الخيارات كالاتى:

[std] تعنى عمليات الاستطلاع التقليدية من ملقم DNS والتي تشمل السجلات الأتية
SOA, NS, A, AAAA, MX and SRV if AXRF on the NS Servers fail.
[rvl] تعنى عملية البحث العكسي.
[brt] تعنى استخدام تقنية brute force.
[srv] للبحث عن سجلات SRV.
[axfr] تستخدم لاختبار ملقم DNS هل تم اعداده بطريقه خاطئة وكان يدعم نقل المنطقة ام لا.
[goo] استخدام محرك البحث جوجل.
[tld] تعنى TOP LEVEL DOMAIN.

```
root@jana:~# dnsrecon.py -t std  -d google.com
[*] Performing General Enumeration of Domain:
[-] DNSSEC is not configured for google.com
[*]      SOA ns1.google.com 216.239.32.10
[*]      NS ns1.google.com 216.239.32.10
[*]      NS ns4.google.com 216.239.38.10
[*]      NS ns3.google.com 216.239.36.10
[*]      NS ns2.google.com 216.239.34.10
[*]      MX alt4.aspmx.l.google.com 74.125.25.27
[*]      MX alt2.aspmx.l.google.com 173.194.69.27
[*]      MX aspmx.l.google.com 173.194.66.27
[*]      MX alt3.aspmx.l.google.com 173.194.71.26
[*]      MX alt1.aspmx.l.google.com 173.194.70.27
[*]      MX alt4.aspmx.l.google.com 2607:f8b0:400e:c03::1a
[*]      MX alt2.aspmx.l.google.com 2a00:1450:4008:c01::1b
[*]      MX aspmx.l.google.com 2a00:1450:400c:c05::1a
[*]      MX alt3.aspmx.l.google.com 2a00:1450:4010:c04::1a
[*]      MX alt1.aspmx.l.google.com 2a00:1450:4001:c02::1b
[*]      A google.com 173.194.45.72
[*]      A google.com 173.194.45.68
[*]      A google.com 173.194.45.73
```

امثله أخرى:

```
dnsrecon.py©-t©std©-d©google.com (Standard (-t std))
dnsrecon.py©-t©tld©-d©google.com (Top Level Domain (-t tld))
dnsrecon.py©-t©axfr©-d©club.net (Zone transfer (-t axfr))
dnsrecon.py©-t©rvl©-i©66.249.92.100,66.249.92.150 (Reverse Record Enumeration (-t rvs))
```

▪ الأداة fierce

قبل الكلام عن هذه الأداة سوف نتكلم أولا ما هو نقل المنطقة zone transfers؟

إذا كان المصطلح **نقل المنطقة** [zone transfer] غير مألوف لك او لا تعرفه، أو لأتعرف الأليات الكامنة وراء تحديثات DNS، فأوصي بشدة أن تقرأ حول هذا الموضوع قبل الشروع في الاستمرار. ويكيبيديا لديها بعض الرؤية في هذا المصطلح من خلال هذا الرابط:

http://en.wikipedia.org/wiki/DNS_zone_transfer (English)
http://support.microsoft.com/kb/164017/ar (Arabic)

المصطلح zone transfer (نقل منطقه او تحويل المنطقة): هو مصطلح يستخدم للإشارة إلى العملية التي يتم نسخ محتويات ملف منطقة DNSمن ملقم DNS أساسي إلى ملقم DNS ثانوي.

نقل المنطقة سيحدث خلال أي من الحالات التالية:

- عند بدء تشغيل خدمة DNS على خادم/ملقم DNS الثانوي.
- عند انتهاء مدة صلاحية وقت التحديث.
- عندما يتم حفظ التغييرات إلى ملف المنطقة الأساسية وهناك "قائمة إعلام".

أساسا، يمكن المقارنة بين نقل المنطقة (zone transfer) وبين استنساخ قاعدة بيانات (database replication) بين خوادم DNS ذات الصلة. عادة ما يتم إجراء تغييرات على ملفات المنطقة على ملقم DNS الأساسي ومن ثم يتم تكرارها من قبل نقل المنطقة (zone transfer) إلى الملقم/الخادم ثانوي.
للأسف، هناك الكثير من المسؤولين الذين يعدون خوادم DNS الخاصة بهم بطريقه خاطئة، ونتيجة لذلك، فان أي شخص يسأل عن الحصول على نسخة من ملقم/خادم DNS يتلقى الطلب. وهذا يعنى تسليم القراصنة التخطيط لشبكة الشركة سواء هيكل الشبكة الخارجية او الداخلية على طبق من فضة.
الان سوف نحاول القيام بعملية نقل المنطقة (zone transfer) للدومين www.offensive-security.com. وذلك باستخدام الامر host او الامر dig في لينكس لمحاولة نقل المنطقة. يمكنك أيضا معرف أسم ملقم/خادم DNS إما باستخدام nslookup أو باستخدام الأمر host.

```
root@jana:~# host -t ns offensive-security.com
offensive-security.com name server ns3.no-ip.com.
offensive-security.com name server ns1.no-ip.com.
offensive-security.com name server ns5.no-ip.com.
offensive-security.com name server ns4.no-ip.com.
offensive-security.com name server ns2.no-ip.com.
root@jana:~#
```

هنا قمنا بمعرفة اسم خادم الأسماء DNS للدومين offensive-security.com وذلك باستخدام الامر host ثم التعبير [-t] الذي يوضع بعده نوع record التي تطلبه وهنا استخدمنا ns أي record الخاص بخادم الأسماء DNS.

```
root@jana:~# host -l offensive-security.com ns4.no-ip.com
; Transfer failed.
Using domain server:
Name: ns4.no-ip.com
Address: 204.16.254.44#53
Aliases:

Host offensive-security.com not found: 5(REFUSED)
; Transfer failed.
root@jana:~#
```

بعد الحصول على اسم خادم الأسماء DNS الخاص بالدومين offensive-security.com قمنا بعمل نقل منطقه (zone transfer) باستخدام الامر host مع التعبير [-l] ولكن نلاحظ ان العملية فشلت. وذلك لان خادم الاسماء الخاص به تم اعداده جيدا.
للمساعد في كتابة أسكر يبات بلغة البايثون حيث تساعدك مباشرة في نقل المنطقة (zone transfer) يمكنك زيارة الرابط التالي:
http://www.dnspython.org/examples.html

كما ناقشنا سابقا، فإن معظم المسؤولين اليوم لديهم ما يكفي من الخبرة لمنع الناس من استكمال نقل المنطقة [zone transfer] غير مصرح بها بشكل عشوائي. ومع ذلك، لم نفقد كل شيء. إذا فشل نقل المنطقة[zone transfer] ، هناك العشرات من الأدوات الجيدة لاستجواب DNS [DNS interrogation]. Fierceهي وسيلة سهلة الاستخدام وعباره عن سكريبت بيرل قوى التي يمكن أن توفر لك العشرات من الأهداف الإضافية. في كالي، يمكنك أن تجد Fierceفي المجلد /usr/bin/. مرة أخرى، يمكنك ببساطة فتح الترمنال وكتابة الأمر "Fierce" (جنبا إلى جنب مع رموز التبديل(التعبيرات) المطلوبة) ولكي تعمل في باك تراك لابد من استدعائها أولا عن طريق الاتي:

Application → backtrack → Information gathering →network analysis →DNS analysis →fierce

يمكن استخدام هذه الطريقة في كالي أيضا كالاتى:

Applications →Kali Linux → Information Gathering → DNS Analysis→ fierce

هذا يطبع رسالة تساعدك على استخدام **fierce** وكيفية تشغيله.

يمكن تثبيتها إذا كنت لا تستخدم نظام تشغيل يدعم هذه الأداة عن طريق [**apt-get install fierce**].

سيبدأ هذا الاسكريبت من خلال محاولة لإكمال نقل المنطقة [**zone transfer**] من الدومين المحدد. في حال فشل هذه العملية، فانه سوف يتحول الى **brute-force host names** وذلك عن طريق إرسال مجموعة من الاستعلامات إلى ملقم **DNS** الهدف. هذا يمكن أن يكون وسيلة فعالة للغاية لكشف أهداف إضافية.

لإجراء فحص لدومين مع الأداة "**fierce**" الذي يستخدم تقنيات مختلفة للعثور على كافة عناوين **IP** وأسماء المضيفين التي يستخدمها الهدف. يمكننا ذلك باستخدام الأمر التالي:

root@kali:~# perl fierce.pl

بما انه سكريبت من النوع بيرل فنقوم بتشغيله على النحو هذا ولكن هذا يؤدى الى ظهور الرسالة التالية:

Can't open perl script "fierce.pl": No such file or directory

هذا ليس جيدا ولكن ماذا حدث. هذه الرسالة تعنى خطأ (**bugs**) وهذا يعنى انه لا يوجد الاسكريبت **fierce**.

```
root@jana:~# locate fierce.pl
root@jana:~# locate fierce
/usr/bin/fierce
/usr/share/applications/kali-fierce.desktop
/usr/share/doc/fierce
/usr/share/doc/fierce/changelog.Debian.gz
/usr/share/doc/fierce/copyright
/usr/share/kali-menu/applications/kali-fierce.desktop
/var/lib/dpkg/info/fierce.list
/var/lib/dpkg/info/fierce.md5sums
root@jana:~#
```

لذلك عند استخدام هذه الأداة نستخدمها كالاتى:

$fierce©-dns©domain_name_on_theinternet.com

بعض المشاكل التي من الممكن ان تقابلك عند استخدام **fierce**في بعض نسخ كالي هو ظهور الرسالة التالية عند استخدام الامر **fierce**.

Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the default wordlist
Exiting...

لحل هذه المشكلة نذهب الى موقع الويب التالي:

http://ha.ckers.org/fierce/hosts.txt

حيث نجد ان هذه عباره عن قائمة من الأسماء تحتوي على **2280** مضيف المشتركة. **Fierce** يستخدم هذه القائمة للبحث عن أسماء مضيف معين ضمن الدومين. بعد ذلك نقوم بالبحث عن نطاق عناوين **IP** ثم نفعل عمليات البحث العكسي لعناوين **IP**. نقوم بنسخ هذا الملف **hosts.txt** في المجلد الحالي (~، المجلد الرئيسي للجذر) وتشغيل **fierce** مرة أخرى.

يمكن استخدام التعبير [**-wordlist**] لتحديد مكان الملف **hosts.txt** الذي تكلمنا عنه من قبل إذا لم يستطع تحديد مكانه.

أيضا يمكن استخدام التعبير [**-file**] لإخراج ناتج البحث في ملف ثم يتبعه اسم الملف الذي تريد حفظ ناتج البحث فيه.

```
root@jana:~# fierce -dns google.com
DNS Servers for google.com:
        ns4.google.com
        ns2.google.com
        ns1.google.com
        ns3.google.com

Trying zone transfer first...
        Testing ns4.google.com
                Request timed out or transfer not allowed.
        Testing ns2.google.com
                Request timed out or transfer not allowed.
        Testing ns1.google.com
                Request timed out or transfer not allowed.
        Testing ns3.google.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2281 test(s)...
173.194.45.84   academico.google.com
173.194.45.80   academico.google.com
173.194.45.81   academico.google.com
173.194.45.83   academico.google.com
```

بعض الأمثلة الأخرى:

fierce©-dns©company.com (Standard Fierce scan)

أسلوب البحث الافتراض لاستخدام الامر **fierce**

fierce©-dns©company.com©-wide (Standard Fierce scan and search all class c ranges found for PTR names that match the domain)

هذا يضمن أسلوب البحث الافتراضي للاداة **fierce** مع بحث لجميع النطاقات من الفئة c وذلن من اجل أسماء **PTR** التي تعادل الدومين

fierce©-dns©company.com©-only©zt (Fierce scan that only checks for zone transfer)

هذا يضمن فقط الفحص من اجل نقل المنطقة (**zone transfer**).

fierce©-dns©company.com©-ztstop (Fierce scan that does not perform brute forcing if a zone transfer is found)

الفحص باستخدام الأداة **fierce** لن يتم استخدام تقنية **brute forcing** إذا كان عملية نقل المنطقة (**zone transfer**) متاحه

fierce©-dns©company.com©-wildcstop (Fierce scan that does not perform bruteforcing if a wildcard is found)

الفحص باستخدام الأداة **fierce** لن يتم استخدام تقنية **brute forcing** إذا وجدت (**wildcard**)

- **الأداة dnsdict6**

هذه الأداة يطلق عليها أيضا **THC-IPV6-ATTACK-TOOLKIT** او **thc-ipv6**. هي أيضا اداه تشابه الأدوات السابقة الذكر في جمع المعلومات من ملقم **DNS**. بمجرد كتابتها في الترمنال بدون أي تعبيرات فانه يعطى جميع المساعدات الممكنة مع هذه الأداة.

فيما يلي طبيعة المعلومات التي يمكن جمعها بواسطة dnsdict6:

- النطاقات الفرعية(**subdomain**).
- عناوين **IP** سواء **IPv4** او**IPv6**.
- سجلات **SRV**.
- سجلات خوادم الأسماء **DNS** [**NS**] وسجلات خوادم البريد الإلكتروني [**MX**].

To open dnsdict6 go to > Kali Linux > Information Gathering > DNS Analysis > dnsdict6

بمجرد فتح**dnsdict6** ، سوف تجد مختلف الخيارات التي تظهر على الشاشة. أفضل اختيار هو اتباع هذه الخيارات، لذلك لا تقم بتشغيل الامر مباشرة، ولكن حاول فهم ما يمكن القيام به بواسطة هذه الخيارات لذلك دعونا نرى فائدة هذه الخيارات مع الأمثلة التوضيحية:

- [-4] البحث عن عناوين**IPv4** – [**dnsdict6©-4©url**]
- [-t©no.] تحدد عدد العمليات التي يمكن القيام بها. العدد الافتراضي هو 8 والحد أقصى هو 32[**dnsdict6©-t18©url**].
- [-d] لعرض معلومات **IPv6** او **IPv4** من سجلات **NS** و **MX** في ملقم الأسماء DNS [**dnsdict6©-d46©URL**].
- [-S] أداء سجلات الخدمة**SRV** .
- [-[smlx]] هذه الخيارات هو لاختيار حجم القاموس يحمل في ثناياه عوامل عده: **s** صغيرة، **m** متوسطة، **l** كبير، **x** اكبر.

```
Syntax: dnsdict6 [-d46] [-s|-m|-l|-x] [-t THREADS] [-D] domain [dictionary-file]

Enumerates a domain for DNS entries, it uses a dictionary file if supplied
or a built-in list otherwise. This tool is based on dnsmap by gnucitizen.org.

Options:
 -4        also dump IPv4 addresses
 -t NO     specify the number of threads to use (default: 8, max: 32).
 -D        dump the selected built-in wordlist, no scanning.
 -d        display IPv6 information on NS and MX DNS domain information.
 -S        perform SRV service name guessing
 -[smlx] choose the dictionary size by -s(mall=50), -m(edium=796) (DEFAULT)
          -l(arge=1416), or -x(treme=3211)
```

1- المثال الأول

استخدامها في عمليات الاستطلاع بالإعدادات الافتراضية كالاتى:

```
root@jana:~# dnsdict6 facebook.com
Starting DNS enumeration work on facebook.com. ...
Starting enumerating facebook.com. - creating 8 threads for 798 words...
Estimated time to completion: 1 to 2 minutes
www.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
blog.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
dns.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
www2.facebook.com. => 2a03:2880:f008:307:face:b00c:0:1
dev.facebook.com. => 2401:db00:10:df02:face:b00c:0:1
new.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
secure.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
login.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
my.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
ca.facebook.com. => 2a03:2880:f008:301:face:b00c:0:1
beta.facebook.com. => 2a03:2880:10:8f11:face:b00c:0:1
```

هنا هو إخراج الأمر الذي يمكن القيام به، فإنه يدل على إدخالات **DNS** مختلفة على الشاشة مع عناوين**IPv6** . يظهر لك هذه الأداة قائمة كبيرة من الإدخالات إذا كان الهدف هو كبير مثل الفيسبوك، وجوجل.

2- المثال الثاني

هنا سوف نقوم بعرض سجلات **DNS** (**NS,MX**) وذلك باستخدام التعبير [**-d**] ونقوم بإضافة **4** اليه اذا كنت تريد العناوين المقابلة له من النوع **IPv4** كالاتى:

```
root@jana:~# dnsdict6 -d4 facebook.com
Starting DNS enumeration work on facebook.com. ...
Gathering NS and MX information...
NS of facebook.com. is a.ns.facebook.com. => 69.171.239.12
NS of facebook.com. is b.ns.facebook.com. => 69.171.255.12
No IPv6 address for NS entries found in DNS for domain facebook.com.
MX of facebook.com. is msgin.t.facebook.com. => 173.252.79.16
No IPv6 address for MX entries found in DNS for domain facebook.com.

Starting enumerating facebook.com. - creating 8 threads for 798 words...
Estimated time to completion: 1 to 2 minutes
ns1.facebook.com. => 69.171.239.12
www.facebook.com. => 31.13.86.49
```

- **الأداة dnsrevenum6**

اداه بسيطة وسريعة وتعتبر أسرع اداه لعملية بحث عكسي باستخدام عناوين IPv6 من ملقم DNS.

dnsrevenum6©dns-server©ipv6address
dnsrevenum6©dns.test.com©2001:db8:42a8::/48

- الأداة dnstracer

Dnstracer تستخدم هذه الأداة في تتبع سلسلة من خوادم DNS إلى المصدر. حيث يحدد من اين يحصل ملقم الاسماء (DNS) على معلوماته ثم يتتبع هذه السلسلة من خوادم **DNS** إلى الخوادم التي تعطيه البيانات.
بمعنى اخر ان تتبع خادم أسماء **DNS** ثانوي حتى يصل الى خادم الأسماء **DNS** الرئيسي الذي هو مصدر المعلومات الرئيسي.

#dnstracer©www.mavetju.org (Search for the A record of www.mavetju.org on your local nameserver)

يستخدم في البحث عن السجل **A** للموقع **www.mavetju.org** من خلال خادم الأسماء **DNS** الخاص بك.

#dnstracer©-s©.©-q©mx mavetju.org (Search for the MX record of mavetju.org on the root-nameserver)

يستخدم في البحث عن السجل **MX** للدومين **mavetju.org** في خادم الأسماء الجذري (**root-nameserver**). التعبير [**-s**] يوضع بعده اسم خادم الأسماء **DNS**الذى تريد البحث فيه عن السجلات. الخيار [**-q**] يوضع بعده نوع السجل الذي تريد ان تبحث عنه.

#dnstracer©-q©ptr©141.230.204.212.in-addr.arpa (Search for the PTR record (hostname) of 212.204.230.141)

يستخدم في البحث عن السجل **PTR** للمضيف وذلك خاص بالعناوين من النوع **IPv4**.

#dnstracer©-q©ptr©-s©.©-o©2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.4.0.2.0.0.0.0.8.b.0.e.f.f.3.ip6.int (for IPv6 addresses)

يستخدم في البحث عن السجل **PTR** للمضيف وذلك خاص بالعناوين من النوع **IPv6**.

▪ Serversniff

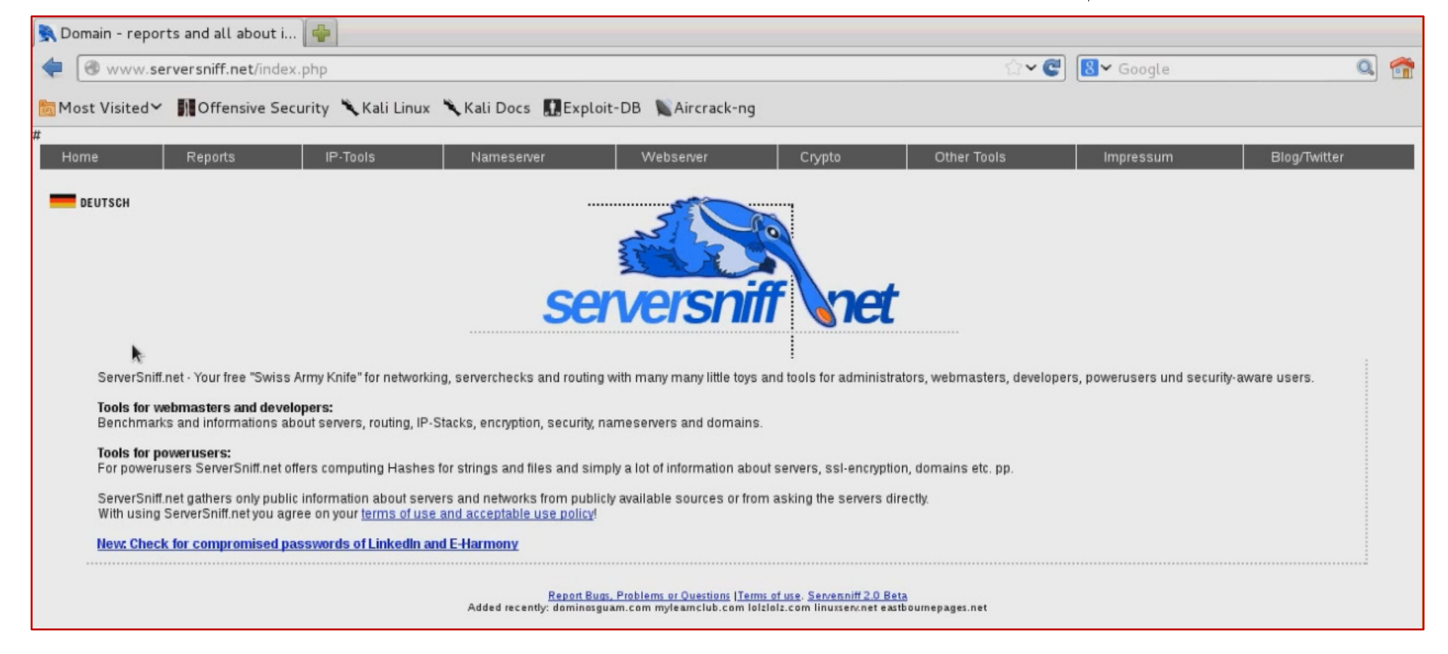
المصدر: **http://www.serversniff.net**

هو موقع ويب يحتوي على العديد من الأدوات التي يمكن استخدامها في جمع المعلومات وتم تقسيم هذه الأدوات في مجموعات كالاتى:

IP tools لجمع كل المعلومات المتعلقة بالعناوين IP

Name Server الخاص بطلبات **DNS**.

Webserver الخاص بالاستعلام عن الدومين و هكذا.



NETWORK FOOTPRINTING-8

الخطوة التالية بعد استرداد معلومات الـ **DNS** هي جمع المعلومات المتعلقة بشبكة الاتصال. لذا، فإننا الآن سوف نناقش عملية الاستطلاع عن الشبكة(network Footprinting) ، والتي تعتبر الوسيلة لجمع المعلومات المتعلقة بالشبكة (network-related information).
يصف هذا المقطع كيفية تحديد نطاق الشبكة (**network range**)، وتحديد نظام التشغيل، والمسار لكي تصل لهذه الشبكة (Traceroute)، وأدوات تتبع المسار.

تحديد نطاق الشبكة (LOCATE NETWORK Range)

لتنفيذ عملية الاستطلاع عن الشبكة**Network Footprinting** فإنك سوف تحتاج إلى جمع المعلومات الأساسية والهامة حول المنظمة الهدف مثل ماذا تفعل المنظمة، الذين يعملون لها وما نوع الأعمال التي يؤدونها. الإجابات على هذه الأسئلة تعطيك فكرة حول الهيكل الداخلي للشبكة الهدف.

بعد جمع المعلومات المذكورة أعلاه، فان المهاجم يمكن المضي قدما للعثور على نطاق الشبكة (**Network Range**) للنظام الهدف. يمكن للمهاجم أيضا الحصول على معلومات أكثر تفصيلا عن قاعدة بيانات السجل الإقليمي بشأن تخصيص **IP** وطبيعة التخصيص (**Regional registry database regarding IP allocation and the nature of the allocation**). يمكن للمهاجم أيضا تحديد الشبكة الفرعية [**subnet mask**] للدومين. يمكن للمهاجم أيضا تتبع الطريق بين النظام الخاص به والنظام الهدف أي بمعنى اخر معرفة جميع اجهز التوجيه **router** التي يمر بها حتى يصل الى الشبكة الهدف. هناك أداتين أكثر شعبية لعملية التتبع (**traceroute tools**) وهي **NeoTrace** و**VisualRoute**. الحصول على عناوين **IP** الخاصة من الممكن ان تكون مفيدة بالنسبة للمهاجمين.

قامت [**IANA**] **The Internet Assigned Numbers Authority** بحفظ الكتل الثلاثة التالية من عنوان **IP** للشبكة الانترنت الخاصة: **10.0.0.0-10.255.255.255(10/8 prefix)**، **172.16.0.0-172.31.255.255 (172.16/12 prefix)** و**192.168.0.0-192.168.255.255 (192.168/16 prefix)**.

نطاق الشبكة يمكنه ان يعطيك فكرة عن كيفية شكل الشبكة، الآلات الموجود في الشبكات على الحالية، وأنه يساعد أيضا على تحديد هيكل الشبكة(**network topology**) ، جهاز التحكم في الوصول، ونظام التشغيل المستخدم في الشبكة الهدف.
للحصول على نطاق الشبكة الخاص بالشبكة الهدف، نقوم بإدخال عنوان **IP** الخاص بالخادم (الذي تم جمعه بواسطة **WHOIS**) في التطبيق **ARIN whois database search tool** أو يمكنك الذهاب إلى الموقع (https://www.arin.net/knowledge/rirs.html) وإدخال الـ **IP** للخادم الهدف في مربع النص **SEARCH Whois**. سوف تحصل على نطاق الشبكة الخاص بالشبكة الهدف. إذا لم يتم اعداد خادم الـ **DNS** بشكل صحيح، فان المهاجم لديه فرصة جيدة للحصول على قائمة بالأجهزة الداخلية على الخادم. أيضا، في بعض الأحيان يمكن للمهاجم تتبع الطريق إلى آلة (**trace a route**)، ومن خلال هذا التتبع فانه يمكنه الحصول على عناوين **IP** الداخلية، والتي قد تكون مفيدة.

Network Whois Record

```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:        207.46.0.0 - 207.46.255.255
CIDR:            207.46.0.0/16
OriginAS:
NetName:         MICROSOFT-GLOBAL-NET
NetHandle:       NET-207-46-0-0-1
Parent:          NET-207-0-0-0-0
NetType:         Direct Assignment
NameServer:      NS2.MSFT.NET
NameServer:      NS4.MSFT.NET
NameServer:      NS1.MSFT.NET
NameServer:      NS5.MSFT.NET
NameServer:      NS3.MSFT.NET
RegDate:         1997-03-31
Updated:         2004-12-09
Ref:             http://whois.arin.net/rest/net/NET-
207-46-0-0-1
OrgName:         Microsoft Corp
OrgId:           MSFT
Address:         One Microsoft Way
City:            Redmond
StateProv:       WA
PostalCode:      98052
Country:         US
RegDate:         1998-07-10
Updated:         2009-11-10
Ref:             http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle:  ABUSE231-ARIN
OrgAbuseName:    Abuse
OrgAbusePhone:   +1-425-882-8080
OrgAbuseEmail:   abuse@hotmail.com
OrgAbuseRef:
http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

ملحوظه: سوف تحتاج الى استخدام أكثر من اداه لجمع المعلومات عن الشبكة حيث استخدام أداة واحده لن يكون لديه المقدرة في جمع المعلومات التي تريدها.

في كالي/باك تراك لينكس

- **الأداة Dmitry:**

هي اداه لديها القدرة على جمع أكبر قدر ممكن من المعلومات عن المضيف. من هذه المعلومات النطاقات الفرعية (**subdomain**)، عناوين البريد الإلكتروني، المعلومات المحدثة، **tcp port scan**، **whois lookups**، وأكثر من ذلك.

توجد في كالي في المسار التالي:

Application → Kali Linux→ Information gathering→ Live Host Identification→ dmitry

```
root@jana:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@jana:~#
```

انظر الى كم التقنيات التي من الممكن ان تؤدى بواسطة هذه الأداة. دعنا نستخدم الامر التالي:

$dmitry©-wnspb©targethost.com©-o©/root/Desktop/dmitry-result

هنا استخدم التعبير [-w] وذلك لعمل **whois lookup** والتعبير [n] لجمع معلومات من **NetCraft** و [s] للبحث عن **subdomain** واستخدم التعبير [o] لوضع ناتج البحث في ملف خارجي وهكذا كما هو موضع في الملف التعريفي.

```
root@jana:~# dmitry -wnspb google.com -o /teba.txt
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to '/teba.txt.txt'

HostIP:173.194.112.71
HostName:google.com

Gathered Inic-whois information for google.com
---------------------------------

   Domain Name: GOOGLE.COM
   Registrar: MARKMONITOR INC.
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: NS1.GOOGLE.COM
```

- **الأداة netmask**

تستخدم لمعرفة نطاق الشبكة لدومين معين كالاتى:

```
root@jana:~# netmask google.com
 173.194.113.65/32
root@jana:~#
```

- **الأداة scapy**

هذه الأداة لها العديد من الوظائف وله أهمية خاصه والتي سوف نتطرق اليها لاحقا ولكن ما يهمنا الان هو جمع المعلومات لنطاق الشبكة باستخدام هذه الأداة يبدا عمل هذه الأداة بكتابة الامر **scapy** في الترمنال فتعمل على انشاء **Interactive shell** اخر كالاتى:

```
root@jana:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>
```

لمعرفة نطاق الشبكة لدومين معين نقوم بإدخال السطر التالي في **Interactive shell** للاداه **scapy** كالاتى:

ans,unans=sr(IP(dst="www.targethost.com/30", ttl=(1,6))/TCP())

```
root@jana:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> ans,unans=sr(IP(dst="www.google.com/30", ttl=(1,6))/TCP())
Begin emission:
.********Finished to send 24 packets.
..........................................................................................
..........................................................................................
```

نقوم بكتابة السطر التالي للحصول على ناتج السطر السابق في جدول كالاتى:

ans.make_table(lambda (s,r): (s.dst, s.ttl, r.src))

```
>>> ans.make_table( lambda (s,r): (s.dst, s.ttl, r.src) )
  173.194.39.20 173.194.39.21 173.194.39.22 173.194.39.23
1 192.168.16.1  192.168.16.1  192.168.16.1  192.168.16.1
2 41.221.137.3  41.221.137.3  41.221.137.3  41.221.137.3
>>>
```

للحصول على **TCP traceroute** مع الأداة **scapy** نكتب السطر التالي:

res,unans=traceroute(["www.google.com","www.Kali-linux.org","www.targethost.com"],dport=[80,443],maxttl=20,retry=-2)

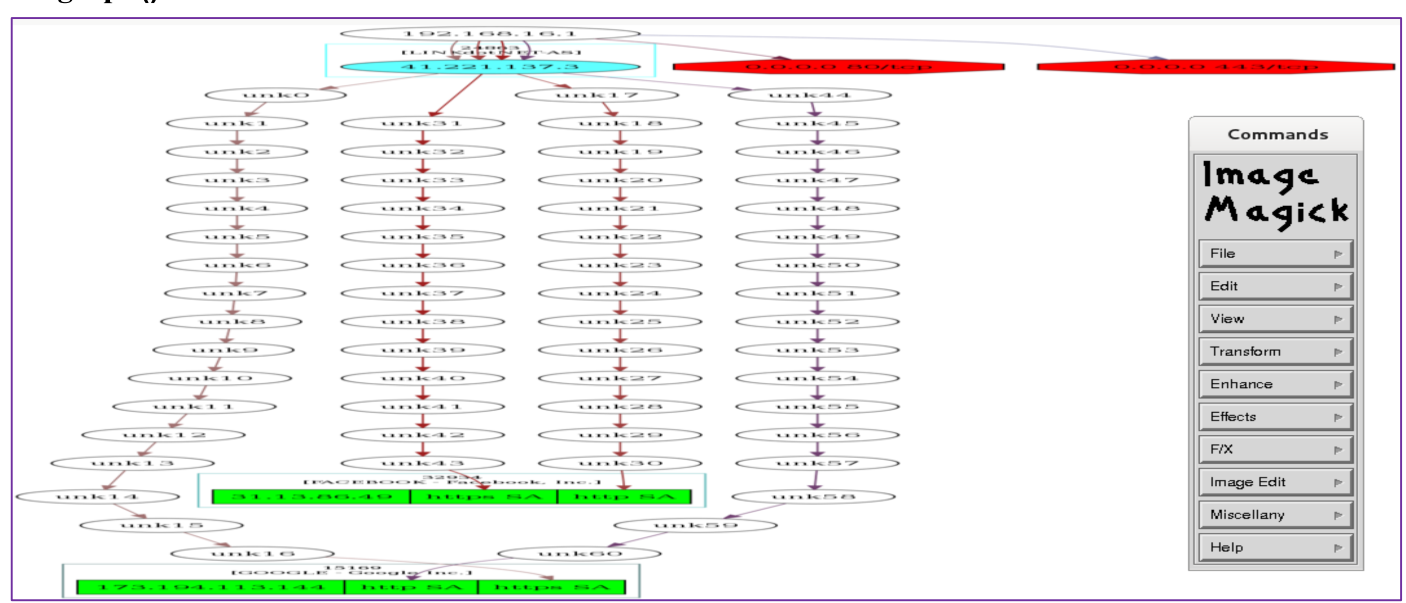
```
>>> res,unans=traceroute(["www.google.com","www.Kali-linux.org","www.facebook.com"],dport=[80,443],maxttl=20,retry=-2
)
Begin emission:
**********Finished to send 120 packets.
*************Begin emission:
Finished to send 99 packets.
.Begin emission:
.Finished to send 99 packets.

Received 23 packets, got 21 answers, remaining 99 packets
   0.0.0.0:tcp443     0.0.0.0:tcp80      173.194.113.144:tcp443 173.194.113.144:tcp80 31.13.86.49:tcp443 31.13.86.49:
tcp80
1  192.168.16.1    11 192.168.16.1    11 192.168.16.1     11     192.168.16.1     11     192.168.16.1     11 192.168.16.1
    11
2  -                  -                  41.221.137.3     11     41.221.137.3     11     41.221.137.3     11 41.221.137.3
    11
16 -                  -                  -                       -                       31.13.86.49      SA -

17 -                  -                  -                       -                       31.13.86.49      SA 31.13.86.49
    SA
18 -                  -                  -                       -                       31.13.86.49      SA 31.13.86.49
    SA
19 -                  -                  -                       -                       31.13.86.49      SA 31.13.86.49
    SA
20 -                  -                  173.194.113.144 SA      173.194.113.144 SA      31.13.86.49      SA 31.13.86.49
    SA
>>>
```

لرؤية النتاج هذا في شكل رسومي نكتب السطر التالي:

res.graph()



ويمكن حفظ الناتج في ملف خارجي باستخدام الصيغة الأتية:

res.graph(target="> /tmp/graph.svg")

للخروج نستخدم الصيغة **exit()**.

تحديد نظام التشغيل (DETERMING THE OPERATING SYSTEM)

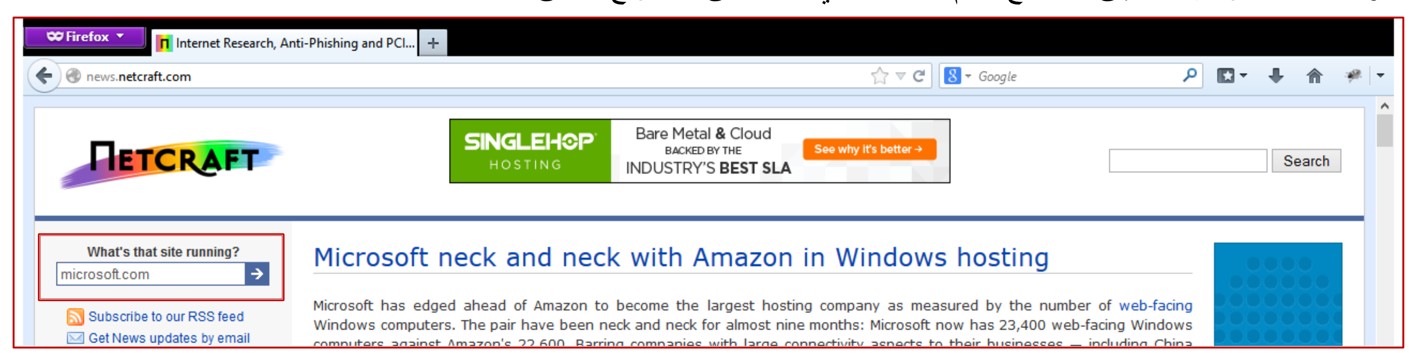
1- NetCraft

المصدر: http://news.netcraft.com

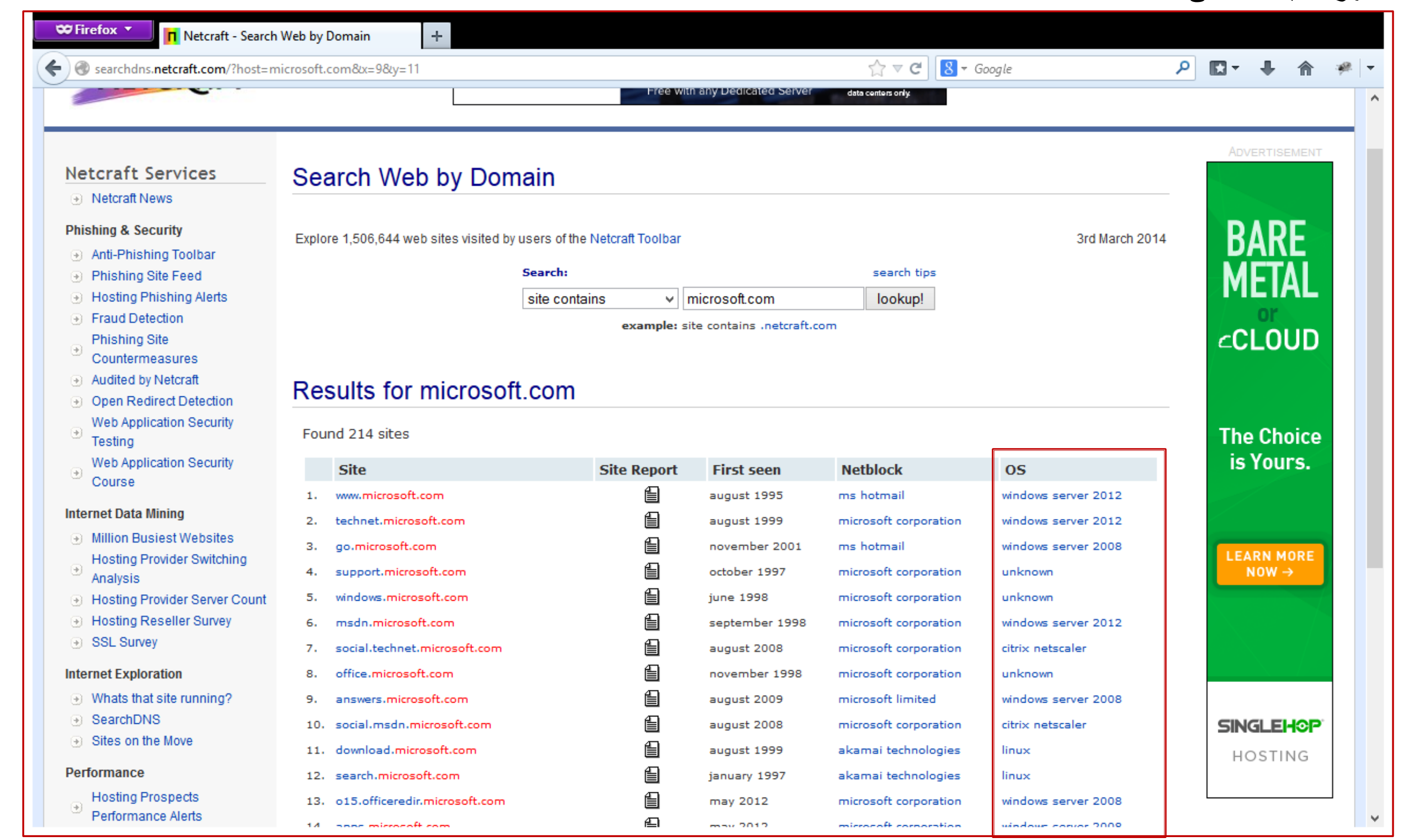
حتى الآن قمنا بجمع المعلومات حول عناوين IP، نطاقات الشبكة، أسماء الخوادم، وما إلى ذلك من الشبكة المستهدفة. الآن حان الوقت لمعرفة نظام التشغيل الذي يعمل في الشبكة الهدف. وتسمى هذه التقنية من الحصول على معلومات حول نظام التشغيل OS الخاص بالشبكة الهدف بـ OS Footprinting. وسوف تساعدك الأداة نيتكرافت على معرفة نظام التشغيل OS قيد العمل على الشبكة الهدف.

نيتكرافت هي شركة لمراقبة الانترنت مقرها في برادفورد أون آفون، انكلترا. أبرز الخدمات التي يتم رصدها هذه الايام هو تقديم كشف عن نظام تشغيل الخادم. نيتكرافت يمكن استخدامها للعثور الغير مباشر عن المعلومات حول خوادم الويب على شبكة الانترنت، بما في ذلك نظام التشغيل الأساسي، نسخة خادم الويب، الرسوم البيانية، وما الى ذلك.

دعونا نرى كيف يساعدانا النيتكرافت في معرفة نظام التشغيل على الشبكة المستهدفة. نقوم بفتح العنوان التالي http://news.netcraft.com في متصفح الويب الخاص بك أي كان نوعه وكتابة اسم الدومين الخاص بالشبكة التي تستهدفها في الحقل **What's that site running?** (هنا سوف نستخدم اسم الدومين microsoft.com على سبيل المثال). فإنه يعرض جميع المواقع المرتبطة بهذا الدومين جنبا إلى جنب مع نظام التشغيل الذي يعمل على كل موقع كالاتي:



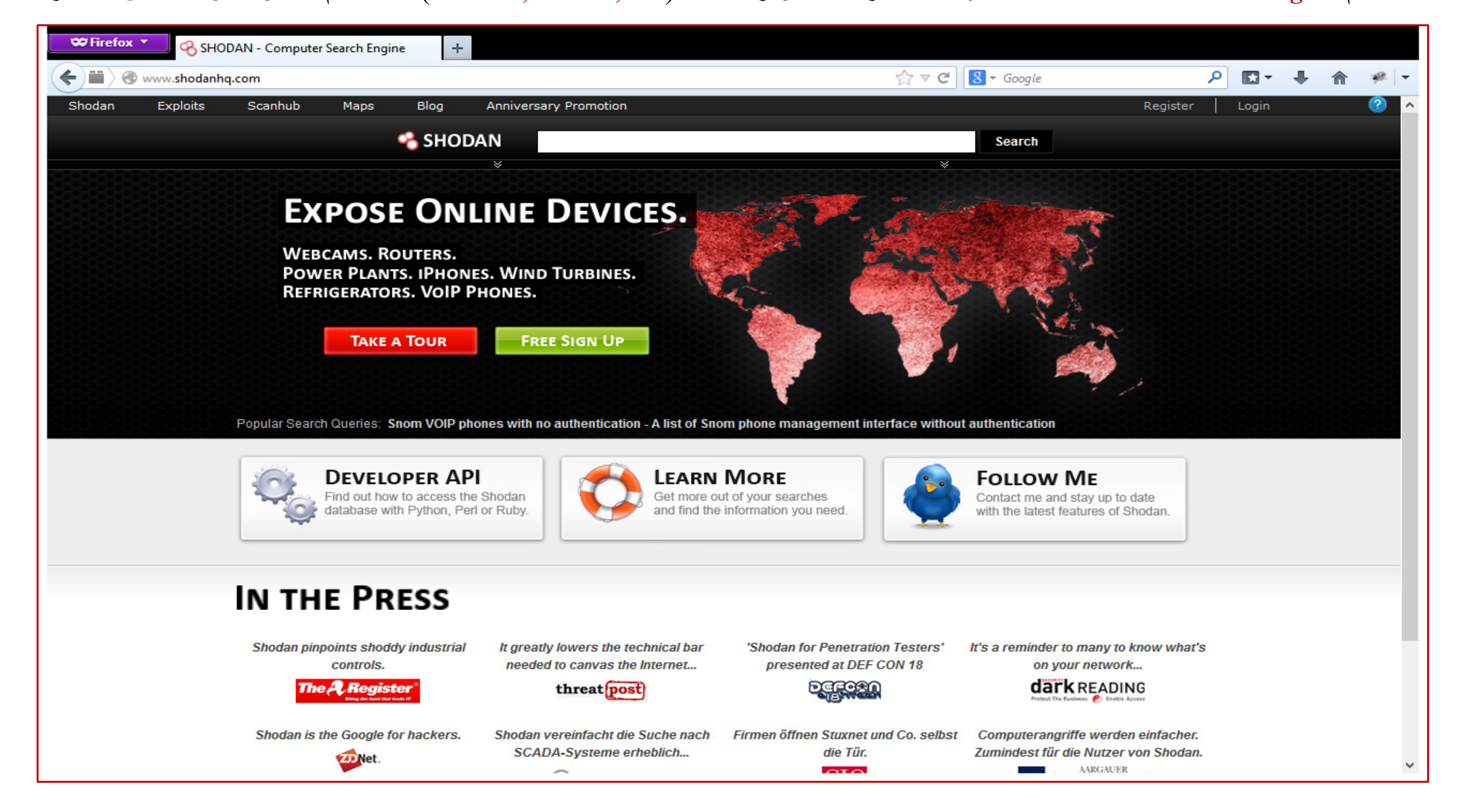
فتظهر النتيجة كالاتي:

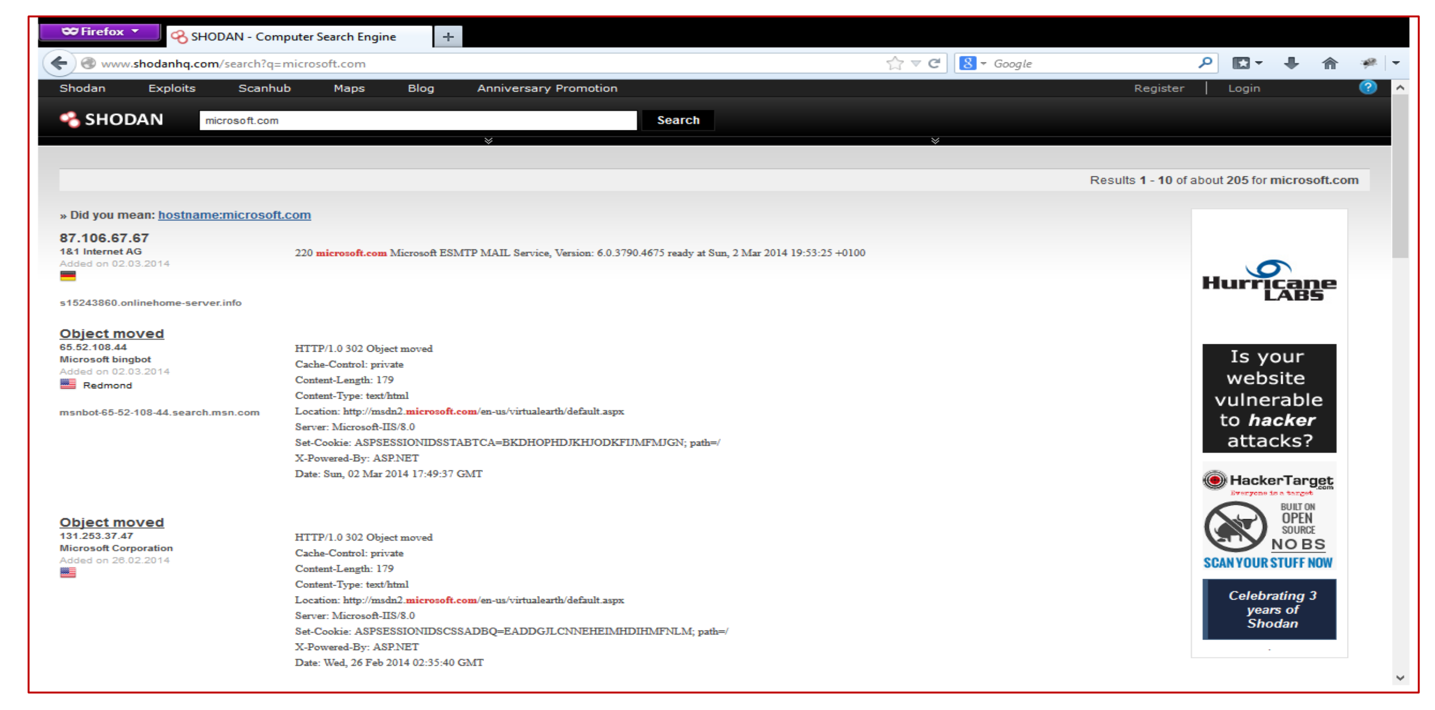


SHODAN Search Engine -2

المصدر: http://www.shodanhq.com

باستخدام SHODAN Search Engine يمكنك إيجاد اجهزه الكمبيوتر الهدف (routers, server, etc) باستخدام مجموعه واسعه من الفلاتر.





TRACEROUTE

العثور على مسار (route)المضيف الهدف (target host) هو ضروري لاختبار ضد الهجمات من النوع [man-in-the middle] والهجمات الأخرى النسبية. وبالتالي، تحتاج إلى العثور على مسار المضيف الهدف في الشبكة. وهذا يمكن أن يتحقق مع مساعدة من أداة تتبع المسار traceroute المقدمة مع معظم أنظمة التشغيل. فإنه يسمح لك بتتبع المسار أو الطريق التي تمر من خلالها الحزم للمضيف الهدف عبر الشبكة.

Traceroute تستخدم مفهوم**ICMP** بروتوكول و **TTL** (**Time to Live**) الموجود في رأس الـ **IP** وذلك للعثور على مسار المضيف الهدف في الشبكة. و هذه الأداة يمكنها عرض التفاصيل حول مسار تحرك الحزم **IP** بين نظامين مختلفين. حيث أنه يمكن أن يعرض لك عدد الموجهات **routers** التي تمر بها الحزم خلال رحلته او تحركه في الشبكة بين النظامين، المدة الزمنية التي تأخذها الحزمة ذهابا وإيابا بين اثنين من أجهزة التوجيه[**routers**]، وإذا كان لدي أجهزة التوجيه إدخالات **DNS**، فانه يعرض أيضا أسماء الموجهات وشبكة الاتصال الخاصة بهم، فضلا عن الموقع الجغرافي.

وهو يعمل عن طريق استغلال ميزة في بروتوكول الإنترنت تسمى **Time to Live** (**TTL**). حيث يتم تفسير الحقل **TTL** للإشارة إلى العدد الأقصى من أجهزة التوجيه التي يمكن للحزمة [**packet**]أن تمر من خلاله. سيكون لكل جهاز **توجيه router**الذي يعالج الحزمة إنقاص مجال العد الخاص بالحقل **TTL** في رأس **ICMP** من جهاز الى اخر او بمعنى اخر ان الحزمة سوف تمر بعدد من اجهز التوجيه لكي تصل اليك من خلال ذلك فان كل جهاز توجيه [**router**] تمر من خلاله سوف يقوم بإنقاص رقم من الحقل **TTL** الموجود في بروتوكول **ICMP** تلو الآخر. عندما يصل العد صفر، سيتم تجاهل الحزمة وستحال رسالة خطأ إلى منشئ الحزمة.

لذلك فان فكرة عمله يقوم عن طريق ارسال حزمه من النوع **ICMP** ويجعل **TTL** الموجود فيه يساوى واحد ويتم ارساله. اول موجه يقابل الحزمة [**First router**] يقوم بخصم رقم واحد من **TTL** فيصبح الرقم صفر وعند ذلك يتم تجاهل الحزمة وارسال رسالة الى الجهاز المضيف انه تم تجاهل الحزمة. هنا يتم تسجيل عناوين **IP** واسم **DNS** الخاص بهذا الموجه (**router**)، ثم يقوم بارسال حزمه أخرى ولكنها هنا تحمل **TTL** يساوى 2 لذلك فان الحزمة يصنع طريقه من خلال الموجه الأول ويتجه الى الموجه الثاني والذي يقوم هو الاخر بتجاهل الحزمة وارسال رسالة الى الجهاز المضيف المنشئ للحزمة انه تجاهل الحزمة. ويستمر في فعل هذا وتسجيل عناوين **IP** واسماء **DNS** الى ان يصل الى الجهاز الهدف او ان يقرر ان الجهاز الهدف من المستحيل ان يصل اليه [**unreachable**]. في هذه العملية، فإنه يسجل الوقت الذي استغرقته كل حزمة في السفر ذهابا وإيابا إلى كل جهاز التوجيه[**router**]. أخيرا، عندما يصل إلى المقصود، فانه سوف يتم إرسال **ICMP ping** العادي إلى المرسل. بالتالي، هذه الأداة تساعد في الكشف عن عناوين **IP** الخاصة بال **hops** الموجودة في المسار التي اتخذته الحزمة لكي يصل الى المضيف الهدف.

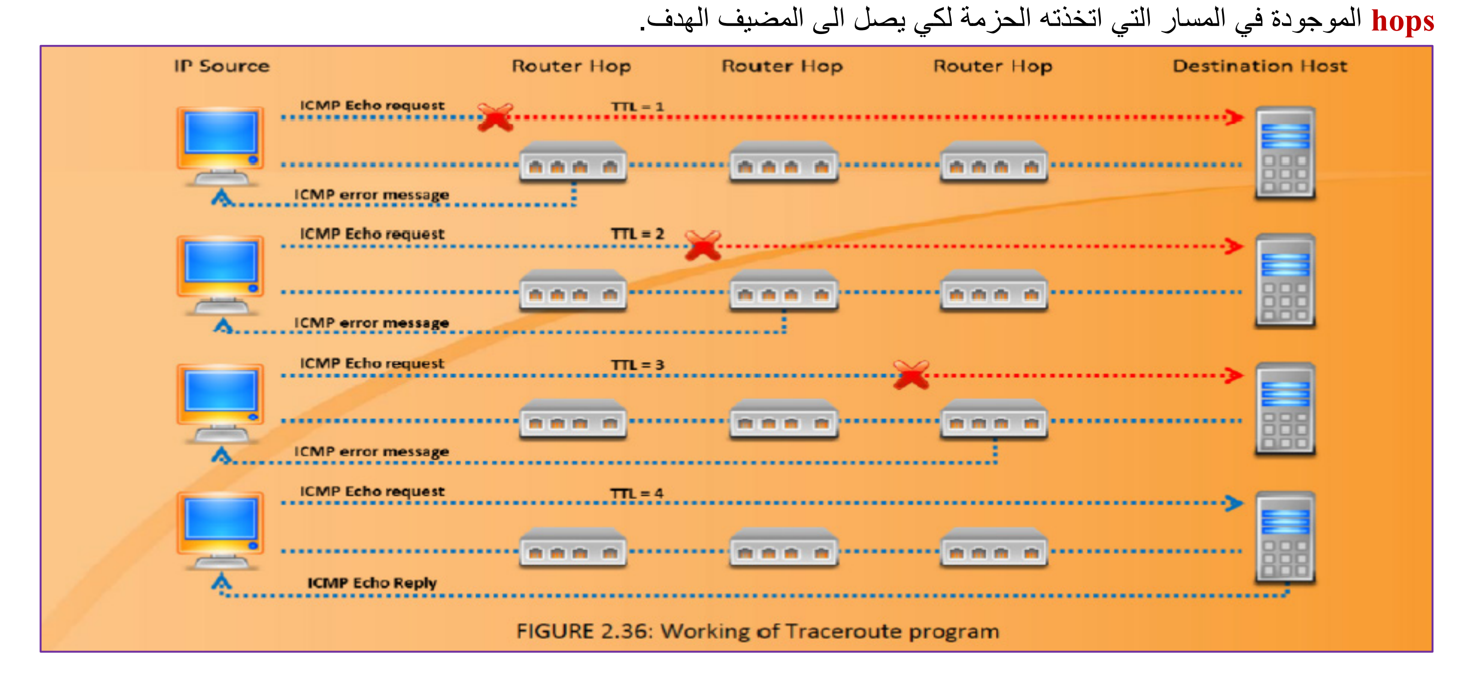


FIGURE 2.36: Working of Traceroute program

كيفية استخدام الامر tracert؟

الذهاب الى **command prompt** في نظام التشغيل ويندوز وكتابة الامر **tracert** متبوعا بعنوان **IP** الهدف او اسم الدومين الهدف كالاتي:

```
C:\>tracert 216.239.36.10
Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:
  1   1262 ms    186 ms    124 ms   195.229.252.10
  2   2796 ms   3061 ms   3436 ms   195.229.252.130
  3    155 ms    217 ms    155 ms   195.229.252.114
  4   2171 ms   1405 ms   1530 ms   194.170.2.57
  5   2685 ms   1280 ms    655 ms   dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
  6    202 ms    530 ms    999 ms   dxb-emix-rb.so100.emix.ae [195.229.0.230]
  7  609 ms   1124 ms   1748 ms   iar1-so-3-2-0.Thamesside.cw.net [166.63.214.65]
```

```
 8 1622 ms   2377 ms   2061 ms   eqixva-google-gige.google.com [206.223.115.21]
 9  2498 ms   968 ms   593 ms   216.239.48.193
 10  3546 ms  3686 ms  3030 ms  216.239.48.89
 11  1806 ms  1529 ms   812 ms  216.33.98.154
 12  1108 ms  1683 ms  2062 ms  ns3.google.com [216.239.36.10]
Trace complete.
```

تحليل ناتج الامر tracert [traceroute analysis]

لقد رأينا كيف يساعدك الأداة **Traceroute** في معرفة عناوين **IP** للأجهزة الوسيطة مثل أجهزة التوجيه**router**، جدران الحماية، وما الى ذلك والذي يوجد بين المصدر والوجهة. هذا يمكنك من رسم الرسم التخطيطي [**topology diagram**] لشبكة الاتصال من خلال تحليل نتائج الأداة **Traceroute**. بعد تشغيل **traceroute** مرات عدة، فإنك سوف تكون قادرا على معرفة موقع أي **HOP** معينة في الشبكة المستهدفة. دعونا ننظر في نتائج **Traceroute** التالية التي تم الحصول عليها:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

من خلال تحليل هذه النتائج، فإن المهاجم يمكنه رسم تخطيطي للشبكة الهدف على النحو التالي:

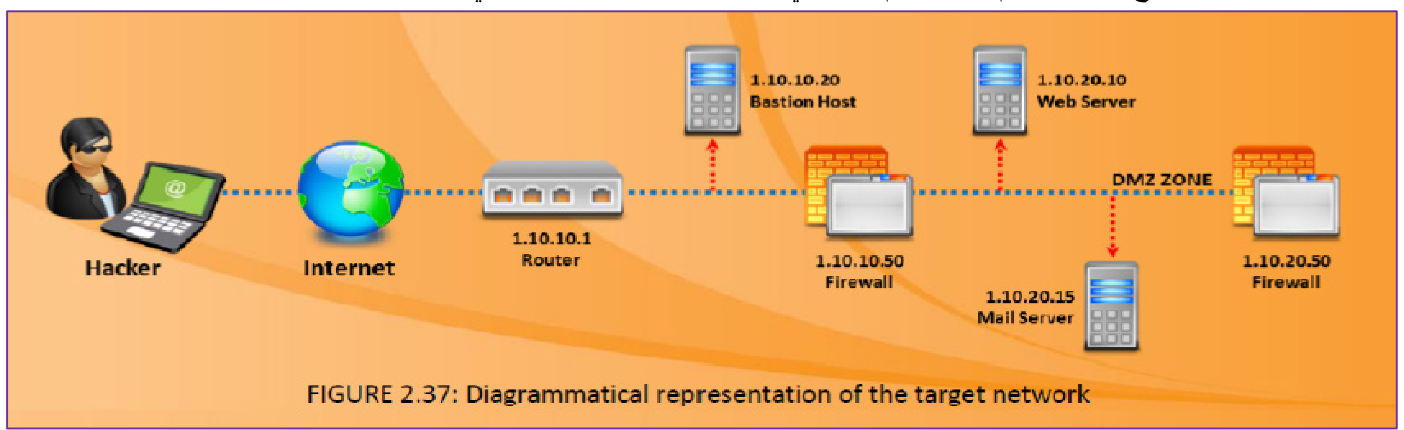


FIGURE 2.37: Diagrammatical representation of the target network

هذا الامر متوفر ايضا في نظام التشغيل لينكس باسم traceroute.

TRACEROUTE TOOLS

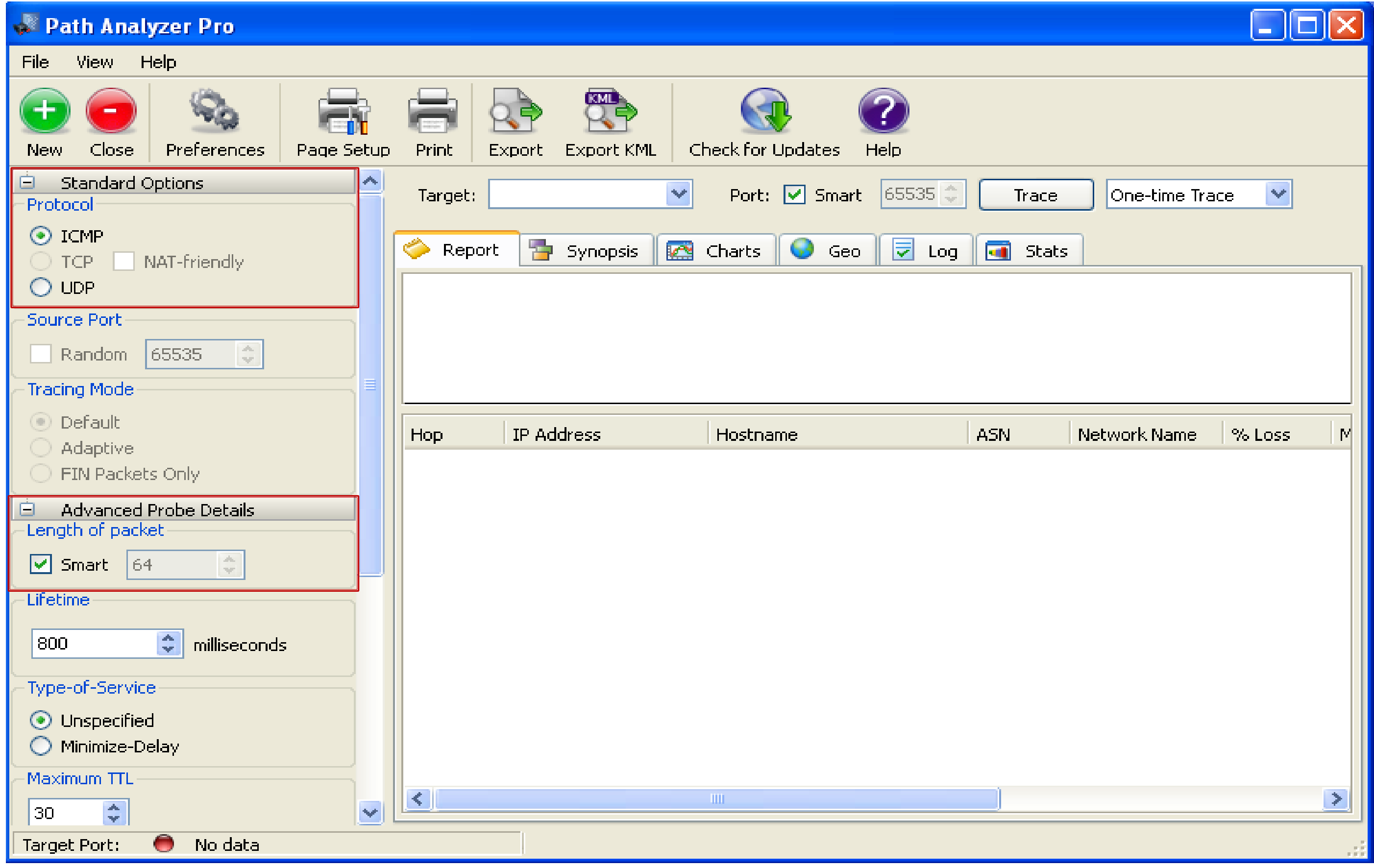
Path Analyzer Pro و**VisuaRoute 2010** هما اداتين يشبهوا في عملهم **Traceroute** وذلك للتتبع مسار الشبكة الهدف.

1- **Path Analyzer Pro**

المصدر: http://www.pathanalyzer.com

Path Analyzer Pro هي أداة ذات وجه رسوميه من النوع **traceroute**والتي تعمل على عرض المسار الذى تتخذه الحزمة من المصدر الى الوجه بطريقه رسوميه. هي تزودك أيضا بمجموعه من المعلومات الأخرى مثل رقم الـ **hop** التي يمر بها وعنوان **IP**الخاص به، واسم المضيف، **ASN**، اسم الشبكة، %LOSS، latency، avg. latency، std. dev. وغيرها من المعلومات الخاصة بكل **hop** يمر به. يمكنك أيضا تحديد موقع الجغرافي للذي يملك عنوان **IP** الموجود في الشبكة الهدف. يمكنه أيضا ان يكشف لك الفلاتر وجدران الحماية وبعض الأشياء الأخرى الموجودة في الشبكة.

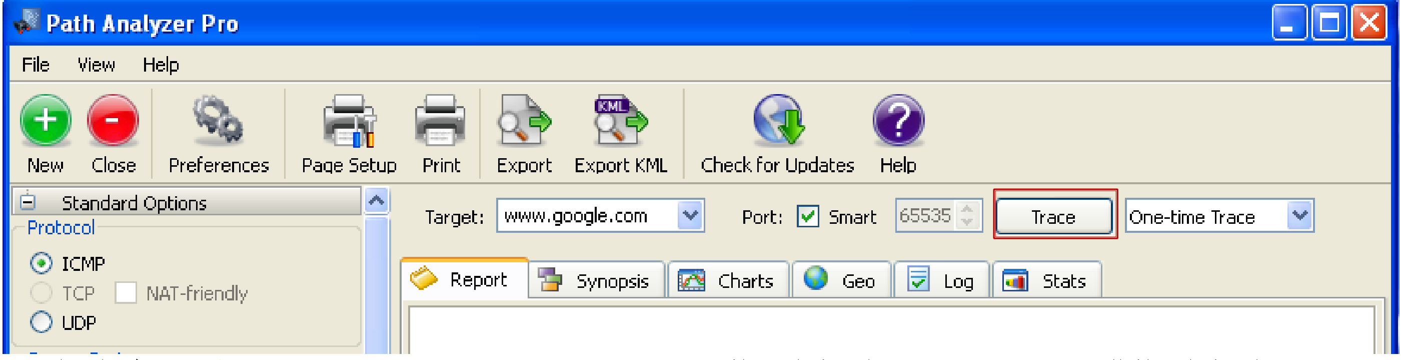
1- نقوم بتثبيته عن طريق اتباع الـ **wizard** الخاص بعملية التثبيت
2- نقوم بفتح البرنامج الان عن طريق الغط مرتين على الأيقونة المعبرة عنه.
3- فتظهر رسالة تريد منك التسجيل فنختار الخيار **Evaluate** لاستخدام النسخة المجانية فتؤدى الى ظهور الشاشة التالية:



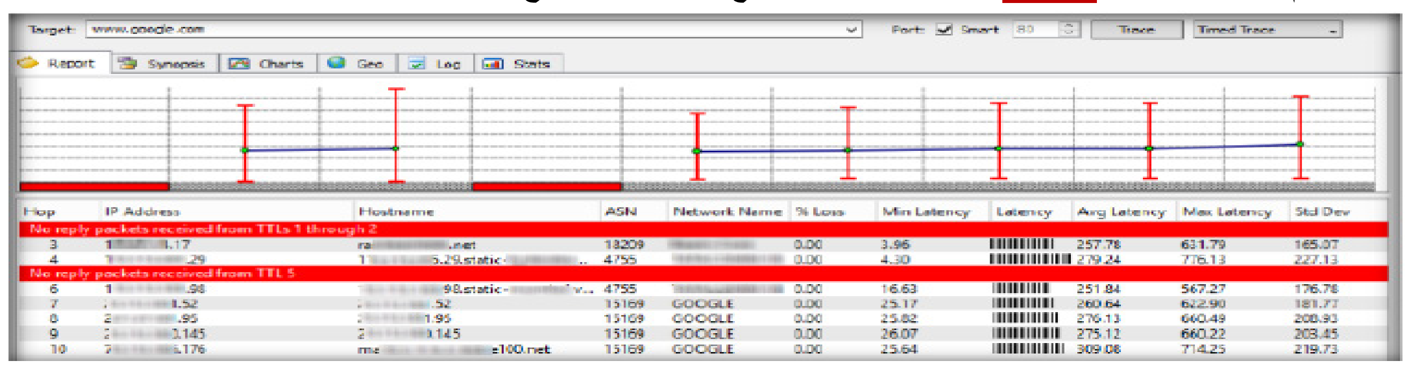
4- في الجزء **Standard Options** نختار **ICMP** وفى الجزء **Advanced Probe Details** نختار **smart** ونترك باقي الخيارات كما هيا.

5- للحصول على نتائج أفضل يجب الغاء تفعيل جدار الحماية لديك.

6- نقوم بكتابة اسم الدومين الهدف في الخانة المقابلة لـ **target** وليكن مثلا www.google.com ويكون كالاتى:

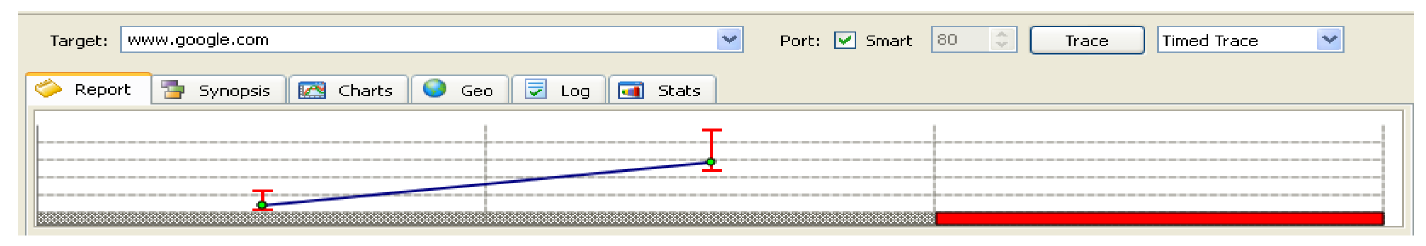


7- في الخانة المقابلة للزر **Trace** نختار من القائمة المنسدلة **Timed Trace** بدلا من **One-time Trace** ثم نضغط على الزر **Trace** فتظهر شاشة أخرى تضع فيها الوقت المستغرق في عملية التتبع وليكن مثلا 3 دقائق حيث يستخدم الشكل HH:MM:SS ثم الضغط على الزر **Accept** بعد الانتهاء من عملية تتبع المسار تظهر النتائج كالاتى:





8- يمكن الضغط على **Report** وذلك ليظهر لك الرسم البياني الخطى لمسار الحزمة من المصدر الى الهدف.
9- يمكن الضغط على **Synopsis** وذلك ليظهر لك ملخص علمية التتبع [**traceroute**].
10- يمكن الضغط على **Charts** وذلك ليظهر لك الرسم البياني لعملية التتبع التي قمت بها.
11- يمكن الضغط على **Geo** وذلك ليظهر لك خريطته تخيليه توضع المسار التي اتخذته الحزمة من المصدر الى الهدف.
12- يمكن حفظ هذه العملية في ملف خارجي عن طريق الضغط على زر **Export**.



ملحوظه هذا التطبيق متوفر أيضا على جميع أنظمة التشغيل الأخرى مثل ماك وجنو/لينكس.

2- VisualRoute 2010

المصدر: **http://www.visualroute.com**

تطبيق اخر قائم على الوجه الرسومية وهي أداة آخري للتتبع تعرض لك تحليل لـ **hop-by-hop**. وأنها تمكنك أيضا من تحديد الموقع الجغرافي للموجهات **routers** والخوادم **server** وأجهزة **IP** الأخرى. أنها قادرة على توفير معلومات التتبع في ثلاثة أشكال: تحليل شامل وعام[**an overall analysis**] ، في جدول بيانات[**in a data table**] ، وكعرض جغرافي للموجهات[**geographical view of the routing**] . جدول البيانات يحتوي على معلومات مثل رقم **hop**، عنوان **IP**، اسم **node** والموقع الجغرافي، وهكذا حول كل مرحلة في الطريق.

المميزات التي يعرضها كالاتى:

[Hop-by-hop traceroutes, Reverse tracing, Historical analysis, Reverse DNS, Ping plotting, Port probing, Firefox and IE plugin]

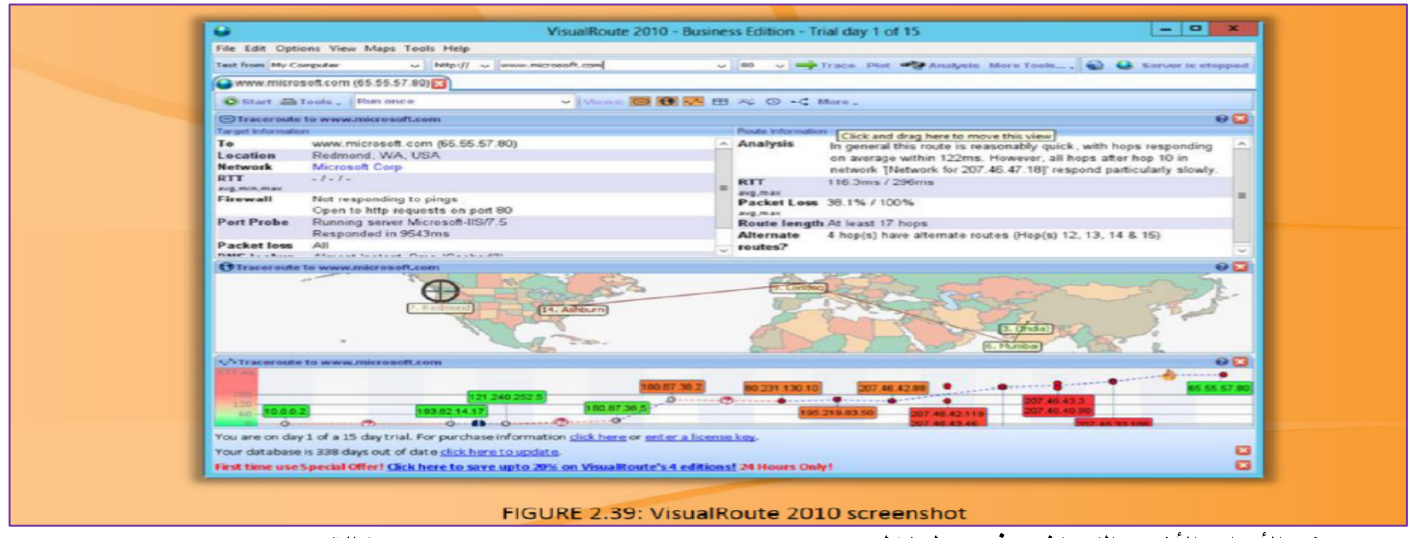


FIGURE 2.39: VisualRoute 2010 screenshot

يوجد بعض الأدوات الأخرى التي تشبه في عملها كل من Path Analyzer Pro وVisualRoute كالاتى:

Network Pinger available at **http://www.networkpinger.com**
GEOSpider available at **http://www.oreware.com**
vTrace available at **http://vtrace.pl**
Trout available at **http://www.mcafee.com**
Roadkil's Trace Route available at **http://www.roadkil.net**
Magic NetTrace available at **http://www.tialsoft.com**
3D Traceroute available at **http://www.d3tr.de**
Analogx HyperTrace available at **http://www.analogx.com**
Network Systems Traceroute available at **http://www.net.princeton.edu**
Ping Plotter available at **http://www.pingplotter.com**



9-عملية الاستطلاع من خلال الهندسة الاجتماعية (FOOTPRINTING THROUGH SOCIAL ENGINEERING)

حتى الآن ناقشنا تقنيات مختلفة لجمع المعلومات إما بمساعدة موارد أو أدوات الإنترنت. الآن سوف نناقش عملية الاستطلاع عن طريق الهندسة الاجتماعية، فن الاستيلاء على المعلومات من الناس عن طريق التلاعب بهم. يغطي هذا القسم مفهوم الهندسة الاجتماعية والتقنيات المستخدمة لجمع المعلومات.

الهندسة الاجتماعية social engineering: هي عملية غير فنية (**non-technical**)تماما والتي يقوم فيها المهاجم بالاحتيال على الشخص الهدف والحصول منه على المعلومات السرية حول الشبكة/المنظمة الهدف مثل هذه الطريقة يكون الشخص الهدف غير مدرك لحقيقة أن شخصا ما يقوم بسرقة المعلومات السرية منه. في الواقع إن المهاجم يلعب لعبة ماكرة مع الهدف من أجل الحصول على معلومات سرية. المهاجم يستفيد من طبيعة مساعدة الناس وضعفهم لتقديم معلومات سرية.

لأداء الهندسة الاجتماعية، عليك أولا كسب ثقة المستخدم المصرح له ثم خداعة للكشف عن المعلومات السرية. الهدف الأساسي من الهندسة الاجتماعية هو الحصول على المعلومات السرية المطلوبة ثم استخدام هذه المعلومات في عملية القرصنة مثل الوصول غير مصرح به إلى النظام[**gaining unauthorized access to the system**] ، سرقة الهوية، التجسس الصناعي، التطفل على الشبكة، ارتكاب عمليات الاحتيال، وما إلى ذلك. من المعلومات التي يتم الحصول عليها عن طريق الهندسة الاجتماعية قد تشمل تفاصيل بطاقة الائتمان، أرقام الضمان الاجتماعي، أسماء المستخدمين وكلمات السر والمعلومات الشخصية الأخرى وأنظمة التشغيل وإصدارات البرامج، عناوين بروتوكول الإنترنت، أسماء الخوادم، معلومات تخطيط الشبكة، وأكثر من ذلك بكثير. المهندسين الاجتماعيين يقوموا باستخدام هذه المعلومات لاختراق النظام أو ارتكاب عمليات احتيال.

الهندسة الاجتماعية يمكن أن توأدي بكثير من التقنيات المختلفة مثل

- التنصت [**eavesdropping**]
- **Shoulder surfing**
- البحث في قمامة المنظمة الهدف(**dumpster diving**)
- الانتحال على مواقع الشبكات الاجتماعية **impersonation on social networking sites**

كما ذكر سابقا **eavesdropping**، **shoulder surfing**، **dumpster driving** هي تقنيات ثلاثة مستخدمة لجمع المعلومات عن طريق الأشخاص الذين يستخدمون الهندسة الاجتماعية. دعونا نناقش هذه التقنيات الخاصة بالهندسية الاجتماعية لفهم الكيفية التي يمكن أن يؤديها في الحصول على معلومات سرية.

EAVESDROPPING (التنصت)

التنصت [eavesdropping]هو فعل الاستماع سرا إلى المحادثات بين الناس سواء من خلال الهاتف أو محادثات الفيديو بدون موافقتهم. يشمل أيضا قراءة الرسائل السرية من وسائط الاتصال مثل الرسائل الفورية أو رسائل الفاكس. بالتالي، فإنه في الأساس فعل اعتراض الاتصالات دون موافقة طرفي الاتصال. مكاسب المهاجم من هذا هو جمع المعلومات السرية من خلال الاستفادة من التنصت على محادثة هاتفية، واعتراض ملفات الصوت والفيديو، أو الاتصال الكتابي.

SHOULDER SURFING

مع هذه التقنية، فإن المهاجم يقف وراء الضحية ويلاحظ أنشطة الضحية على الكمبيوتر مثل ضربات المفاتيح أثناء إدخال أسماء المستخدمين وكلمات السر وغيرها سرا.

يستخدم هذا الأسلوب عادة للحصول على كلمات السر، **PINs**، الرموز الأمنية، أرقام الحسابات، معلومات بطاقة الائتمان، وبيانات مماثلة. فإنه يمكن أن يؤديها في مكان مزدحم لأنه من السهل نسبيا الوقوف وراء الضحية دون معرفته.

DUMPSTER DIVING

هذه التقنية معروف أيضا باسم **trashing**، حيث يقوم المهاجم بالحصول على المعلومات من القمامة الخاصة بالشركة الهدف. قد يحصل المهاجم على معلومات حيوية مثل فواتير الهاتف، معلومات الاتصال، المعلومات المالية والمعلومات المتعلقة بالعمليات، مطبوعات للكود المصدري (**printouts of source code**)، مطبوعات من المعلومات الحساسة، وغيرها من المعلومات وذلك من صناديق القمامة الخاصة بالشركة الهدف، وصناديق القمامة الخاصة بالطابعة، ملاحظات لاصقة في مكاتب المستخدمين، وما إلى ذلك من المعلومات التي تم الحصول عليها يمكن أن تكون مفيدة للمهاجمين لارتكاب عملية القرصنة.

10-عمليات استطلاع من خلال شبكات التواصل الاجتماعي [FOOTPRINTING THROUGH SOCIAL NETWORKING SITE]

على الرغم من ان عملية الاستطلاع من خلال مواقع الشبكات الاجتماعية تبدو مماثلة لعملية الاستطلاع عن طريق الهندسة الاجتماعية، ولكن هناك بعض الاختلافات بين الطريقتين. في عملية الاستطلاع عن طريق الهندسة الاجتماعية، فان المهاجم يحتال على الناس للكشف عن المعلومات في حين أنه في عملية الاستطلاع من خلال مواقع الشبكات الاجتماعية، فان المهاجم يجمع المعلومات المتاحة من خلال مواقع الشبكات الاجتماعية. حيث يمكن للمهاجمين استخدام مواقع الشبكات الاجتماعية كوسيلة لتنفيذ هجمات الهندسة الاجتماعية. ويوضح هذا القسم كيف وماذا يمكن جمعه من المعلومات من مواقع الشبكات الاجتماعية عن طريق الهندسة الاجتماعية.

عملية الاستطلاع باستخدام الهندسة الاجتماعية من خلال مواقع التواصل الاجتماعي

مواقع الشبكات الاجتماعية هي خدمات عبر الإنترنت اونلاين، المنصات، أو المواقع التي تسمح للناس بالتواصل مع بعضهم البعض، وبناء العلاقات الاجتماعية بين الناس. استخدام مواقع الشبكات الاجتماعية في تزايد سريع. أمثلة على مواقع الشبكات الاجتماعية تشمل **Facebook**، **Myspace**، **LinkedIn**، **Twitter**، **Pinterest**، **google+**، وهلم جرا. كل مواقع الشبكات الاجتماعية لديها أغراضها ومميزاتها الخاصة. قد يكون القصد موقع واحد للاتصال بالأصدقاء والأسرة وغيرها، وآخر قد يكون القصد لتبادل التشكيلات المهنية وغيرها ومواقع الشبكات الاجتماعية مفتوحة للجميع. المهاجمون قد يستفيدون من هذا لانتزاع المعلومات الحساسة من المستخدمين إما عن طريق التصفح من خلال لمحات عامة عن المستخدمين أو عن طريق خلق صورة وهمية وخداع المستخدم للاعتقاد انه مستخدم حقيقي.
هذه المواقع تسمح للناس بالبقاء على اتصال مع الآخرين، الحفاظ على الشخصية المهنية، وتبادل المعلومات مع الآخرين. على مواقع الشبكات الاجتماعية، يقوم الناس بنشر معلومات مثل تاريخ الميلاد، المستوى التعليمي، خلفيه عن العمل، أسماء الزوجين، وغيرها. الشركات قد تنشر معلومات مثل الشركاء المحتملين، والمواقع، والأخبار القادمة عن الشركة.
بالنسبة للمهاجمين، فان مواقع الشبكات الاجتماعية يعتبر مصدرا كبيرا للعثور على معلومات عن الشخص الهدف أو الشركة. هذه المواقع تساعد مهاجم لجمع المعلومات فقط التي تم تحميلها من قبل الشخص أو الشركة. المهاجمين يمكنهم بسهولة الوصول إلى الصفحات العامة لهذه الحسابات. للحصول على مزيد من المعلومات حول الهدف، فان المهاجمين يقومون بإنشاء حسابات وهمية واستخدام الهندسة الاجتماعية لإغراء الضحية للكشف عن مزيد من المعلومات. على سبيل المثال، يمكن للمهاجم إرسال طلب صداقة إلى الشخص الهدف من حساب وهمي، وإذا قبل الضحية الطلب، فان المهاجم يمكنه الوصول الى صفحات محدودة عن الشخص المستهدف على هذا الموقع. وبالتالي، فان مواقع الشبكات الاجتماعية يمكنها ان تكون مصدرا قيما للمعلومات عن المهاجمين.

المعلومات المتاحة على مواقع التواصل الاجتماعي (INFORMATION AVAILABLE IN THE SOCIAL NETWORKING SITE)

حتى الآن، لقد ناقشنا كيف يمكن للمهاجم انتزاع المعلومات من مواقع الشبكات الاجتماعية، والآن سوف نناقش ما هي المعلومات التي يمكن للمهاجم الحصول عليها من مواقع الشبكات الاجتماعية.
الناس عادة يقوم بإنشاء صفحه شخصيه على مواقع التواصل الاجتماعي من أجل توفير المعلومات الأساسية عنهم وللحصول على علاقة مع الآخرين. يحتوي الملف الشخصي عموما على بعض المعلومات مثل الاسم ومعلومات الاتصال (رقم الهاتف النقال، البريد الإلكتروني)، معلومات الأصدقاء، معلومات عن أفراد الأسرة، اهتماماتهم، والأنشطة، الخ. الناس عادة يرتبطون بأصدقائهم ويقومون بالدردشة معهم. يمكن للمهاجمين جمع المعلومات الحساسة من خلال الأحاديث الخاصة بهم. مواقع الشبكات الاجتماعية يسمح أيضا لناس بمشاركة الصور والفيديو مع أصدقائهم. إذا كان الناس لا يقومون بتعيين إعدادات الخصوصية الخاصة بهم لألبوماتهم، فان المهاجمين يمكنهم الاطلاع على الصور ومقاطع الفيديو المشتركة من قبل الضحية. يمكن للمستخدمين الانضمام إلى مجموعات للعب الألعاب أو لتبادل وجهات النظر والاهتمامات. المهاجمون يمكنهم انتزاع المعلومات حول اهتمامات الضحية من خلال تتبع مجموعاته ثم يمكنه ان يحتال على الضحية للكشف عن مزيد من المعلومات. يمكن للمستخدمين إنشاء أحداث لإعلام المستخدمين الآخرين حول المناسبات القادمة. مع هذه الأحداث، يمكن المهاجمين كشف أنشطة الضحية. بالنسبة للأفراد، والمنظمات يمكنهم ان يستخدموا مواقع التواصل الاجتماعي للتواصل مع الناس، والترويج لمنتجاتهم، وجمع الملاحظات حول منتجاتهم أو خدماتهم، الخ.
أنشطة المنظمة على مواقع التواصل الاجتماعي والمعلومات ذات الصلة التي يمكن للمهاجم انتزاعها هي كما يلي:

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Background check to hire employees	Type of business

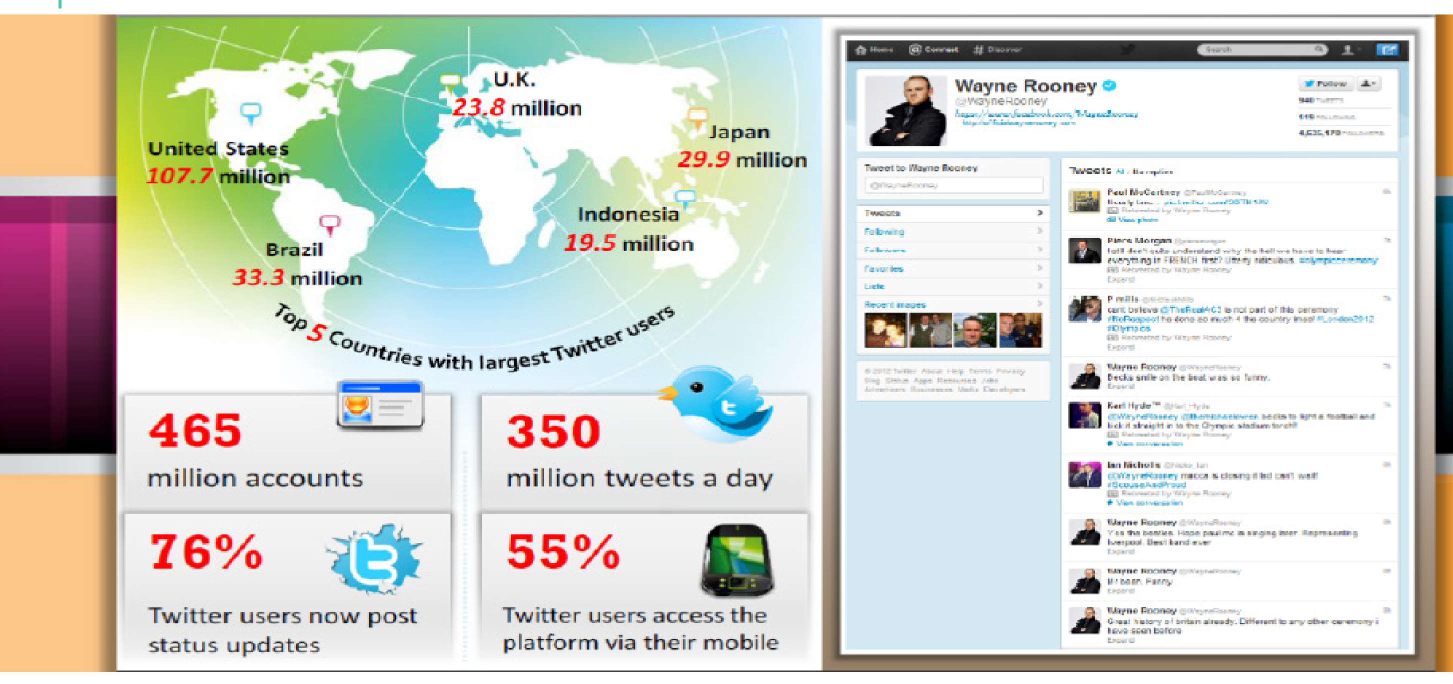
TABLE 2.1: What organizations Do and What Attacker Gets

جمع المعلومات عن طريق الفاسبوك [COLLECTION FACEBOOK INFORMATION]



الفاسبوك هو واحد من أكبر مواقع التواصل الاجتماعي في العالم، حيث يملك أكثر من 845،000،000 مستخدم نشط شهريا في جميع أنحاء العالم. أنه يتيح للناس إنشاء الصفحة الشخصية الخاصة بهم، إضافة الأصدقاء، تبادل الرسائل الفورية، إنشاء أو الانضمام إلى مجموعات أو مجتمعات مختلفة، وأكثر من ذلك بكثير. يمكن للمهاجم الاستيلاء على جميع المعلومات التي قدمتها الضحية في الفاسبوك. لانتزاع المعلومات من الفاسبوك، ينبغي أن يكون للمهاجم حساب نشط. المهاجم يقوم بتسجيل الدخول للحساب الخاص به، يقوم بالبحث عن الشخص المستهدف أو المنظمة. تصفح الملف الشخصي للشخص الهدف قد يكشف الكثير من المعلومات المفيدة مثل رقم الهاتف، رقم البريد الإلكتروني، الأصدقاء، التفاصيل التعليمية، التفاصيل المهنية، الاهتمامات، الصور، وأكثر من ذلك بكثير. يمكن للمهاجم استخدام هذه المعلومات لمزيد من التخطيط لعملية القرصنة، مثل الهندسة الاجتماعية، للكشف عن مزيد من المعلومات حول هذا الهدف.

جمع المعلومات عن طريق التوتير [COLLECTION TWITTER INFORMATION]



تويتر هو موقع تواصل الاجتماعي اخر ذات شعبيه كبرى يستخدمها الناس لإرسال وقراءة الرسائل النصية[text-based messages] . فإنه يسمح لك بتتبع أصدقائك، والخبراء والمشاهير المفضلين لك، وما الى ذلك. هذا الموقع أيضا يمكن أن يكون مصدرا كبيرا للمهاجمين للحصول على معلومات حول الشخص الهدف. هذا مفيد في استخراج المعلومات مثل المعلومات الشخصية، معلومات الاصدقاء، أنشطة الشخص الهدف التي تم نشرها باسم تويت، اما الذي يتبعه الهدف [following]، المستخدمين الذين يتبعون الهدف، الصور التي يتم تحميلها، وما إلى ذلك. المهاجم قد يحصل على معلومات مفيدة من تويت المستخدم الهدف.

جمع المعلومات عن طريق LINKEDIN [COLLECTION LINKEDIN INFORMATION]



على غرار الفاسبوك وتويتر، LinkedIn هو موقع آخر للتواصل الاجتماعي للمتخصصين professionals. أنه يتيح للناس لإنشاء وإدارة صفحته الشخصية وتعريفها. أنه يسمح للمستخدمين لبناء والانخراط مع شبكتهم المهنية. بالتالي، فإن هذا يمكن أن يكون مصدر معلومات كبير بالنسبة للمهاجم. المهاجم قد يحصل على معلومات مثل تفاصيل التوظيف الحالية وتفاصيل العمل الماضية وتفاصيل التعليم، وتفاصيل الاتصال، وأكثر من ذلك بكثير عن الشخص الهدف. المهاجم يمكنه جمع كل هذه المعلومات مع عملية الاستطلاع [Footprinting].

جمع المعلومات عن طريق يوتيوب [COLLECTION YOUTUBE INFORMATION]



اليوتيوب هو موقع ويب على شبكة الانترنت يتح لك رفع ومشاهدة ملفات الفيديو ومشاركة من خلال العالم كله. المهاجم يمكنه عن طريق اليوتيوب البحث عن جميع ملفات الفيديو المرتبطة بالهدف ومن خلالها جمع المعلومات عنه.

TRACKING USERS ON SOCIAL NETWORKING SITES (تتبع المستخدمين على مواقع التواصل الاجتماعي)

من أجل حماية أنفسنا من الاحتيال عبر الإنترنت والهجمات، فان الأشخاص الذين يعانون من المعرفة القليلة حول جرائم الإنترنت يستخدمون هويات وهمية على مواقع التواصل الاجتماعية. في مثل هذه الحالات، فإنك لن تحصل على معلومات دقيقة عن المستخدم الهدف. لذلك لتحديد الهوية الحقيقية للمستخدم الهدف، يمكنك استخدام أدوات مثل Get Someone's IP or IP-GRABBER لتتبع الهويات الحقيقية للمستخدمين.

إذا كنت تريد أن تتبع هوية مستخدم معين، فانه يجب عليك القيام بما يلي:

- قم بفتح متصفح الويب لديك ثم قم بطبع عنوان **URL** التالي فيه:

http://www.myiptest.com/staticpages/index.php/how-about-you

- نلاحظ الحقول الثلاثة الموجودة في الجزء السفلي من صفحة الويب، **Link for person**، **Redirect URL: http://** أو **Link for you**.

Find / Get someones IP Address

Can I get someones IP Address ?
The answer is both yes and maybe, and it may not do you any good. Try this tool to find someones IP Address.

Link for person: http://www.myiptest.com/img.php?id=u3bdquryey&rdr=www.g

Redirect URL: http:// www.gmail.com

Link for you:
http://www.myiptest.com/staticpages/index.php/how-about-you?id=u3bdquryey&show_ip=1

Topics
What's this (FAQ)

Friend Sites
Hosting
Neighbors

Blacklist IP check

1- للحصول على عنوان الـ **IP** الحقيقي الخاص بالهدف، قم بنسخ الرابط المنشأ والموجود في الحقل **Link for person** وإرساله إلى الهدف عن طريق الدردشة.

2- ندخل أي عنوان **URL** خاص بالهدف في الحقل **Redirect URL: http://** ليتم توجيهه.

3- فتح عنوان **URL** الموجودة في الحقل **Link for you** في صفحة آخري، لرصد تفاصيل عنوان IP الهدف وتفاصيل إضافية.

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

FIGURE 2.44: Tracing identity of user's

2.4 أدوات عملية الاستطلاع FOOTPRINTING TOOLS

Footprinting يمكن القيام بها عن طريق مساعدة من الأدوات. العديد من المنظمات تقدم الأدوات التي تجعل جمع المعلومات مهمة سهلة. هذه الأدوات ضمان الحد الأقصى من المعلومات التي يمكن جمعها. في هذا الجزء سوف يتم شرح استخدام هذه الأدوات في جمع المعلومات من مصادر مختلفة.

FOOTPRINTING TOOL: MALTEGO

المصدر: **http://paterva.com**

في نظام التشغيل ويندوز

Maltego هو تطبيق مفتوحة المصدر يتميز بالذكاء وتطبيق الطب الشرعي[**intelligence and forensics application**] . يمكن استخدامه لمرحلة جمع المعلومات لجميع الأعمال المتصلة بالأمن[**Security related work**] . **Maltego** هو عبارة عن منصة وضعت لتقديم صورة واضحه للتهديدات الممكنة على البيئة التي تملكها وتديرها منظمة ما. يمكن أن تستخدم لتحديد العلاقات والروابط في العالم الحقيقي بين الناس، الشبكات الاجتماعية، الشركات والمؤسسات والمواقع الإلكترونية، والبنية التحتية للإنترنت (الدومين وأسماء **DNS**، **Netblocks**، عناوين **IP**)، والعبارات[**phrases**]، والانتماءات[**affiliations**]، والوثائق، والملفات.



Internet Domain



Personal Information

FIGURE 2.45: Maltego showing Internet Domain and personal information

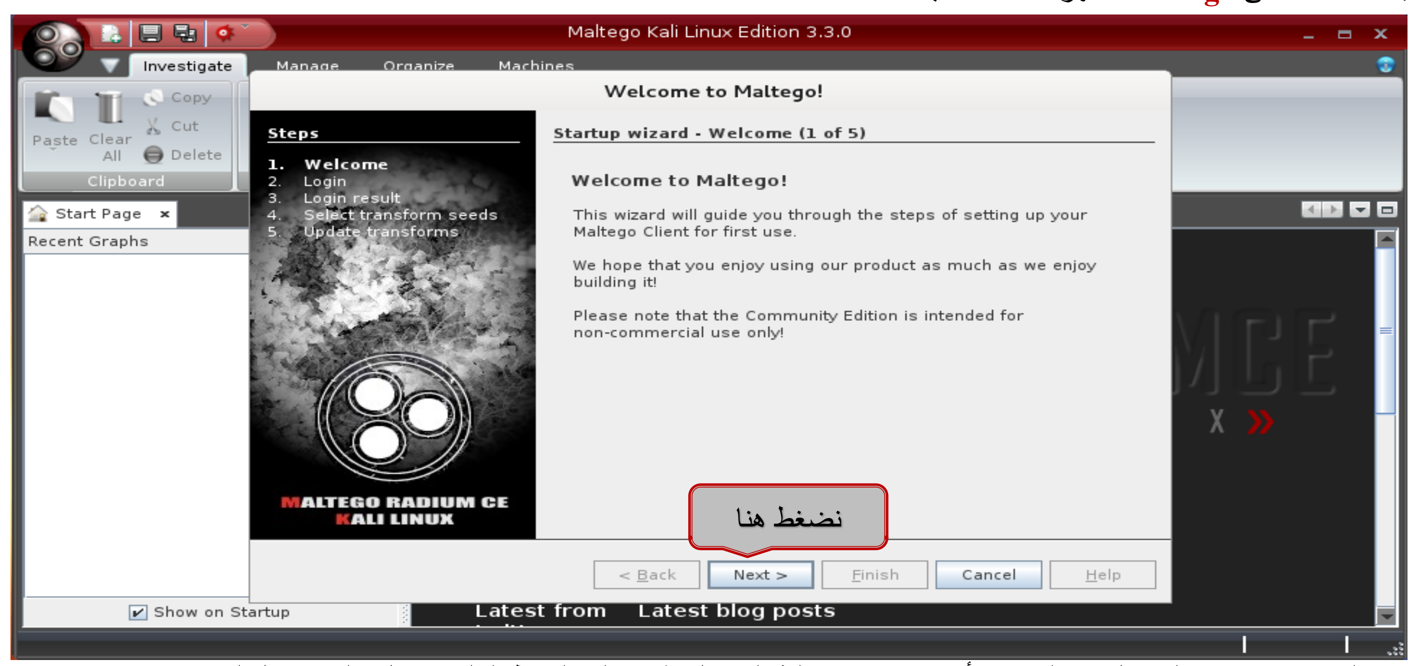
Maltego هي أداة استطلاع بنيت في كالي/باك تراك من قبل **Paterva**. هي أداة استطلاع متعددة الأغراض التي يمكن جمع المعلومات المفتوحة والعامة على شبكة الإنترنت. لديه إمكانيات استطلاع **DNS**، ولكنه يذهب أعمق من ذلك بكثير في عمليات جمع المعلومات. فإنه يأخذ المعلومات ويعرض النتائج في الرسم البياني للتحليل.

لبدء **Maltego**، انتقل إلى قائمة **Application** في كالي، وانقر على القائمة كالي. ثم حدد

Information Gathering → DNS Analysis → Maltego

الخطوة الأولى لاستخدام **Maltego** هو التسجيل فيه. لا يمكنك استخدام التطبيق من دون التسجيل.

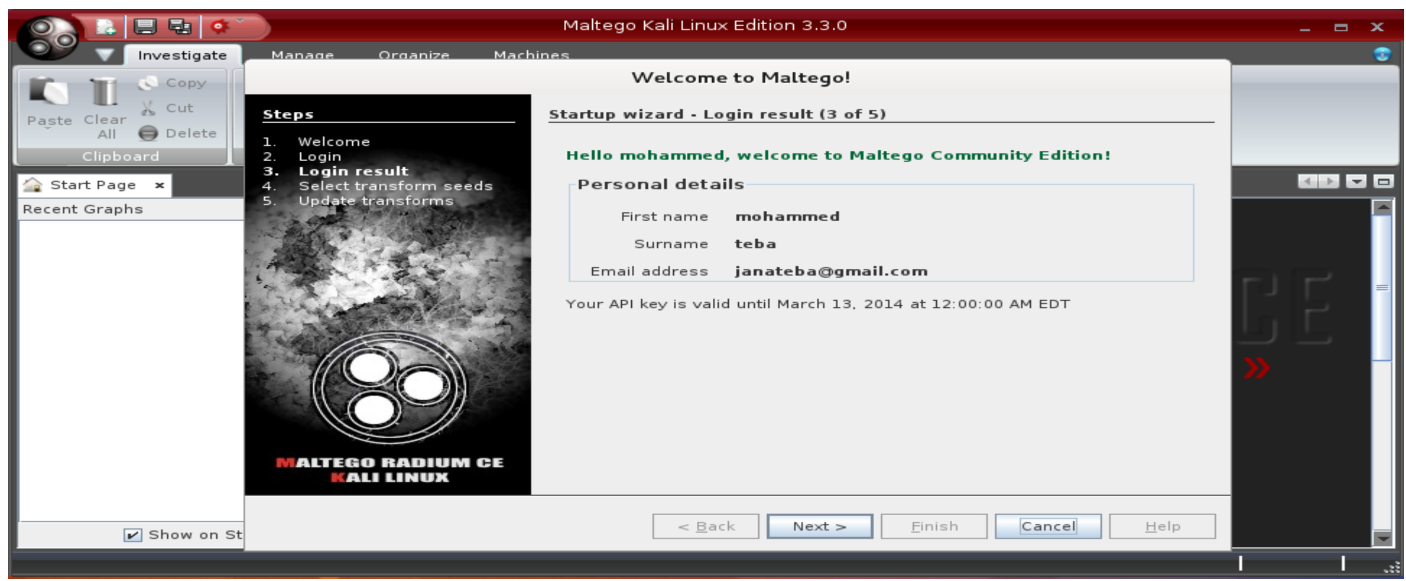
بعد الضغط على **Maltego** تظهر الشاشة التالية:



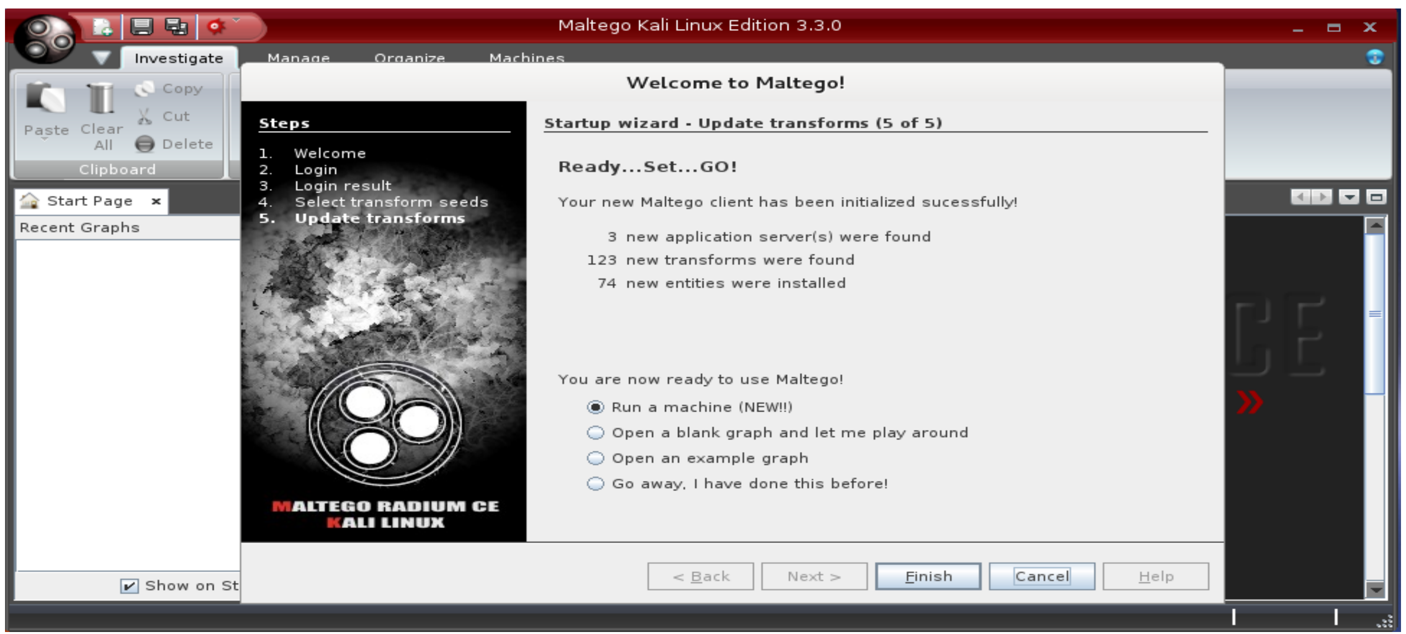
كما قلنا سابقا لابد من التسجيل في البرنامج أولا ولإجراء عملية التسجيل نذهب الى الرابط التالي ونعمل على تسجيل لبياناتنا فيه:

https://www.paterva.com/web6/community/maltego/





ثم نضغط **next** حتى تصل الى الشاشة التالية ثم نضغط **Finish** كالاتي:



Maltego لديه طرق عدة لجمع المعلومات. أفضل طريقة لاستخدام **Maltego** هو الاستفادة من معالج بدء التشغيل (**run a machine**) لتحديد نوع المعلومات التي ترغب في جمعها. المستخدمين ذوي الخبرة قد يريدون أن يبدأ مع رسم بياني فارغة (**open a blank graph**) أو تخطى هذا ال **wizard**. قوة **Maltego** هو أنه يتيح لك مراقبة بصريه للعلاقة بين الدومين، والمنظمة، والناس. يمكنك التركيز حول منظمة معينة، أو نظرة على منظمه والشراكات ذات الصلة من استعلامات **DNS**.

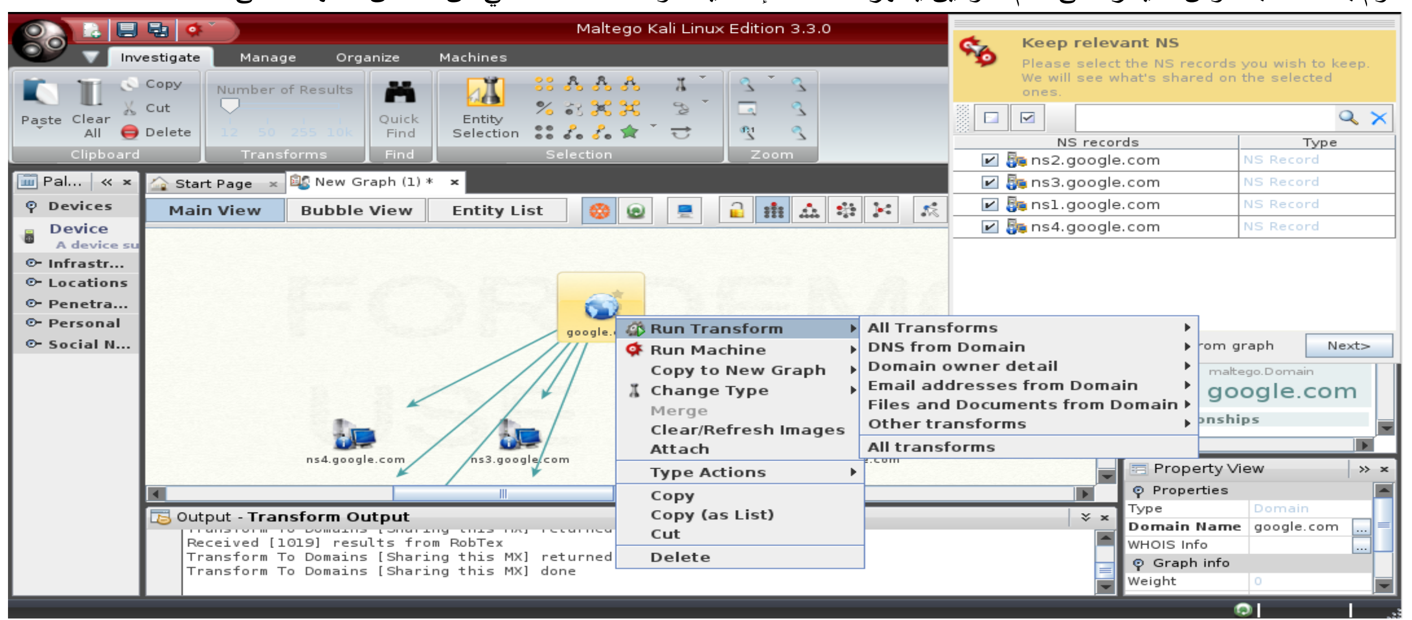
اعتمادا على خيارات الفحص المختارة فان Maltego يمكنه أداء المهام التالية:

1- [**Associate an e-mail address to a person**] ضم عناوين البريد الإلكتروني للأشخاص.
2- [**Associate websites to a person**] ضم مواقع الويب للأشخاص.
3- [**Verify an e-mail address**] التحقق من البريد الإلكتروني.
4- [**Gather details from Twitter, including geo location of pictures**] جمع المعلومات من تويتر، بما في ذلك تحديد الموقع الجغرافي للصور.
5- جمع ارقام التليفونات والكثير من المعلومات عن طريق استخدامه محركات البحث.

ملحوظه: هذا التطبيق من اهم التطبيقات في جمع المعلومات.

معظم الميزات لا تحتاج إلى تفسير، وتشمل كيفية استخدامها تحت وصف الميزة. ويستخدم عادة **Maltego** في جمع المعلومات واستخدامها في بعض الأحيان كخطوة أولى خلال هجوم الهندسة الاجتماعية.

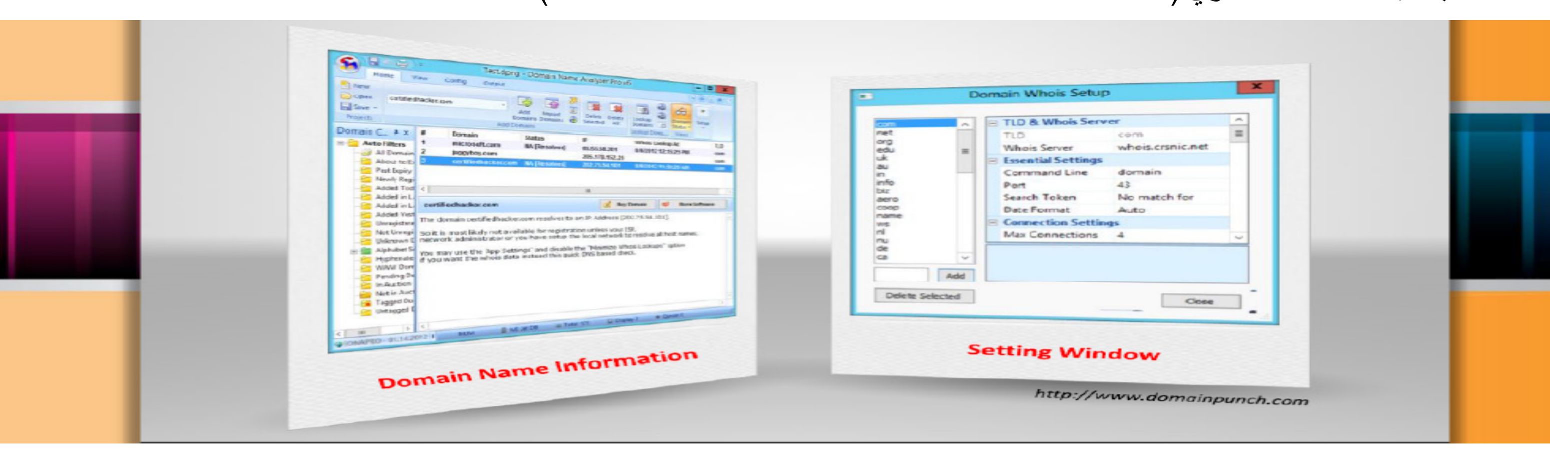
نقوم بالضغط بالماوس الايسر على اسم الدومين يظهر مختلف الإمكانيات والاستعلامات التي من الممكن ادائها كالاتى:



FOOTPRINTING TOOL: DOMAIN NAME ANALYZER PRO

المصدر: http://www.domainpunch.com

Domain Name Analyzer Professional هو برنامج على نظام التشغيل ويندوز لإيجاد وإدارة والحفاظ على أسماء الدومين المتعددة. انها تدعم عرض البيانات الإضافية (expiry and creation dates, name server information)، علامات الدومين، عمليات بحث **whois** الثانوي (for thin model whois TLDs مثل COM، NET، TV).



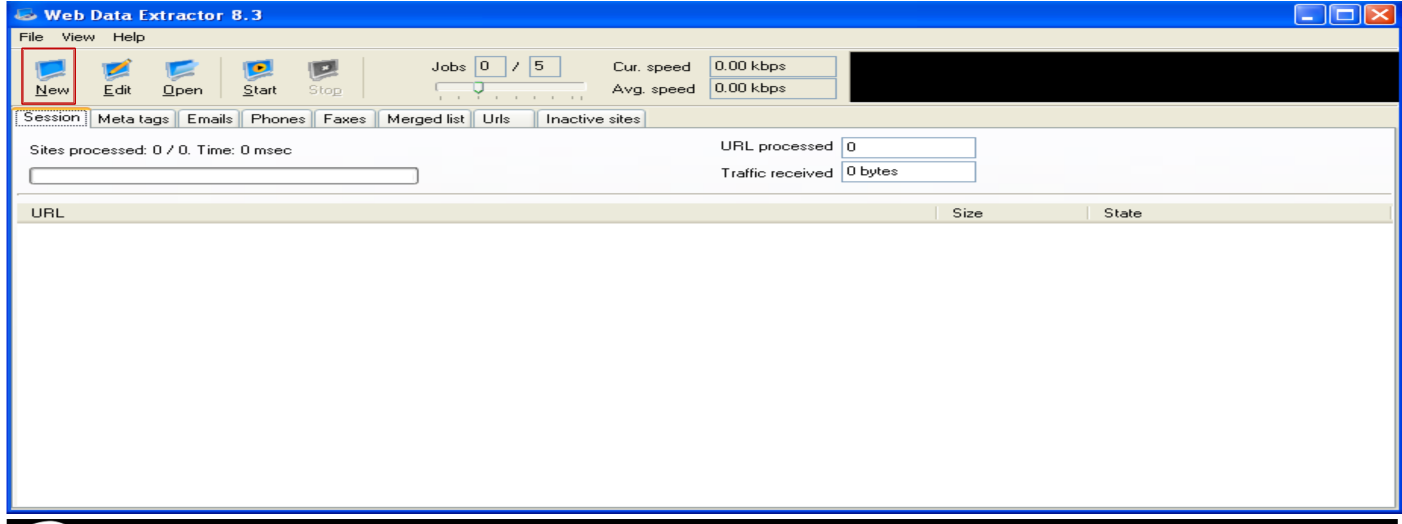
FOOTPRINTING TOOL: WEB DATA EXTRACTOR

المصدر: http://www.webextractor.com

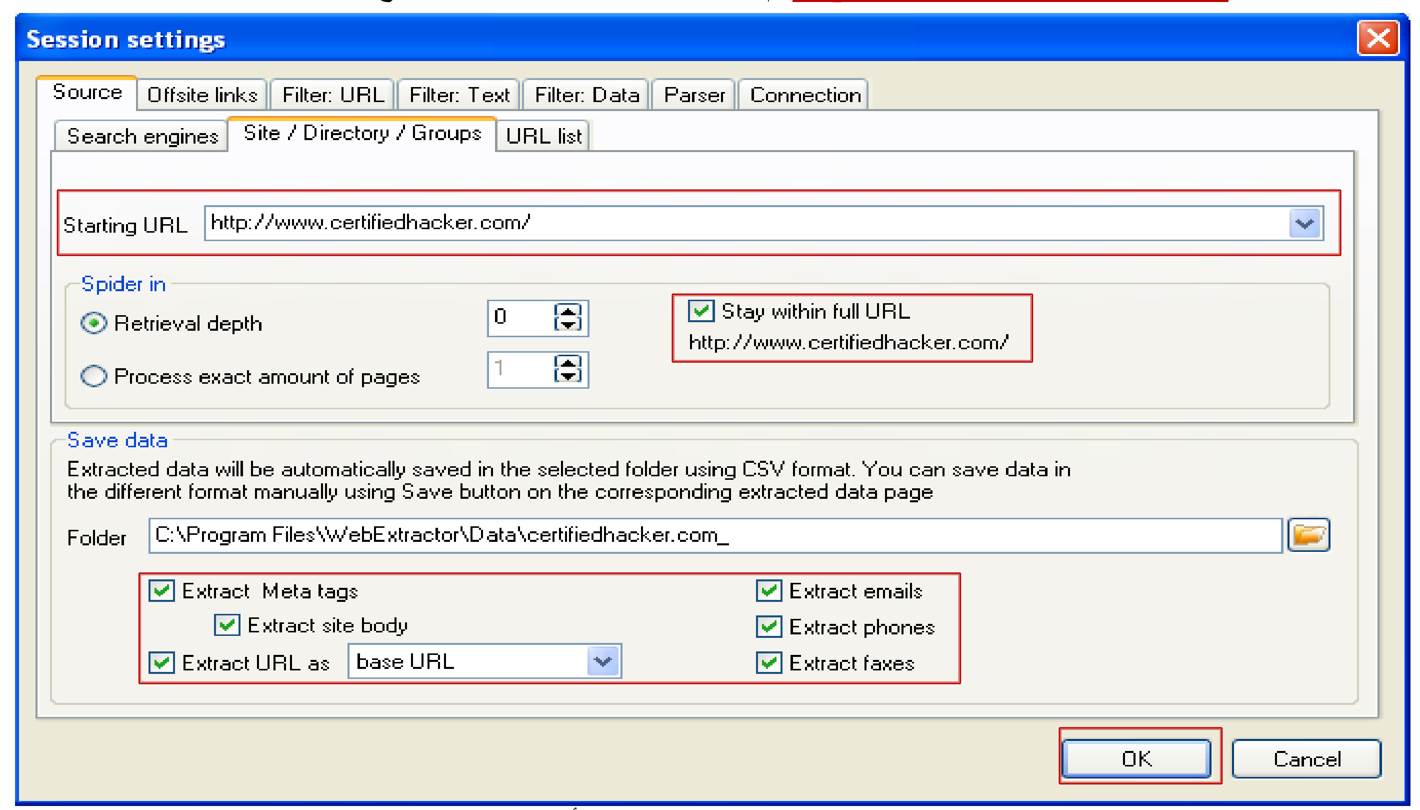
Web Data Extractor هو أداة لاستخراج البيانات. فإنه يعمل على استخراج بيانات الاتصال للشركة الهدف (البريد الإلكتروني، والهاتف، والفاكس) من شبكة الإنترنت. يعمل على استخراج عناوين **URL** والعلامة الوصفية meta tag(العنوان)، desc، الكلمة الرئيسية) لتعزيز الموقع، يبحث عن منشئ الدومين، وما إلى ذلك.

المهاجمون يبحثوا باستمرار عن أسهل الطرق لجمع المعلومات. هناك العديد من الأدوات المتاحة للمهاجمين التي بواسطتها يمكنهم استخراج قاعدة بيانات الشركة. بمجرد الوصول إلى قاعدة البيانات، فإنه يمكن أن يجمع عناوين الموظفين، البريد الإلكتروني، أرقام الهواتف، عناوين المواقع الداخلية في الشركة، وهكذا. مع هذه المعلومات التي تم جمعها فانه يمكن إرسال رسائل البريد الغير مرغوبة[**spam email**] للموظفين لملء صندوق البريد الخاص بهم، اقتحام المواقع الإلكتروني للشركة، تعديل عناوين المواقع الداخلية. كما أنها قد تثبت بعض الفيروسات الخبيثة لجعل قاعدة البيانات غير صالحة للعمل. باعتبارك مختبر اختراق، فانه يجب عليك أن تكون قادرا على التفكير من وجهة نظر القرصان ومحاولة غلق كل السبل الممكنة لجمع المعلومات عن المنظمات. يجب أن تكون قادرا على جمع كل المعلومات السرية لتنظيم وتنفيذ ميزات الأمان لمنع تسرب بيانات الشركة.

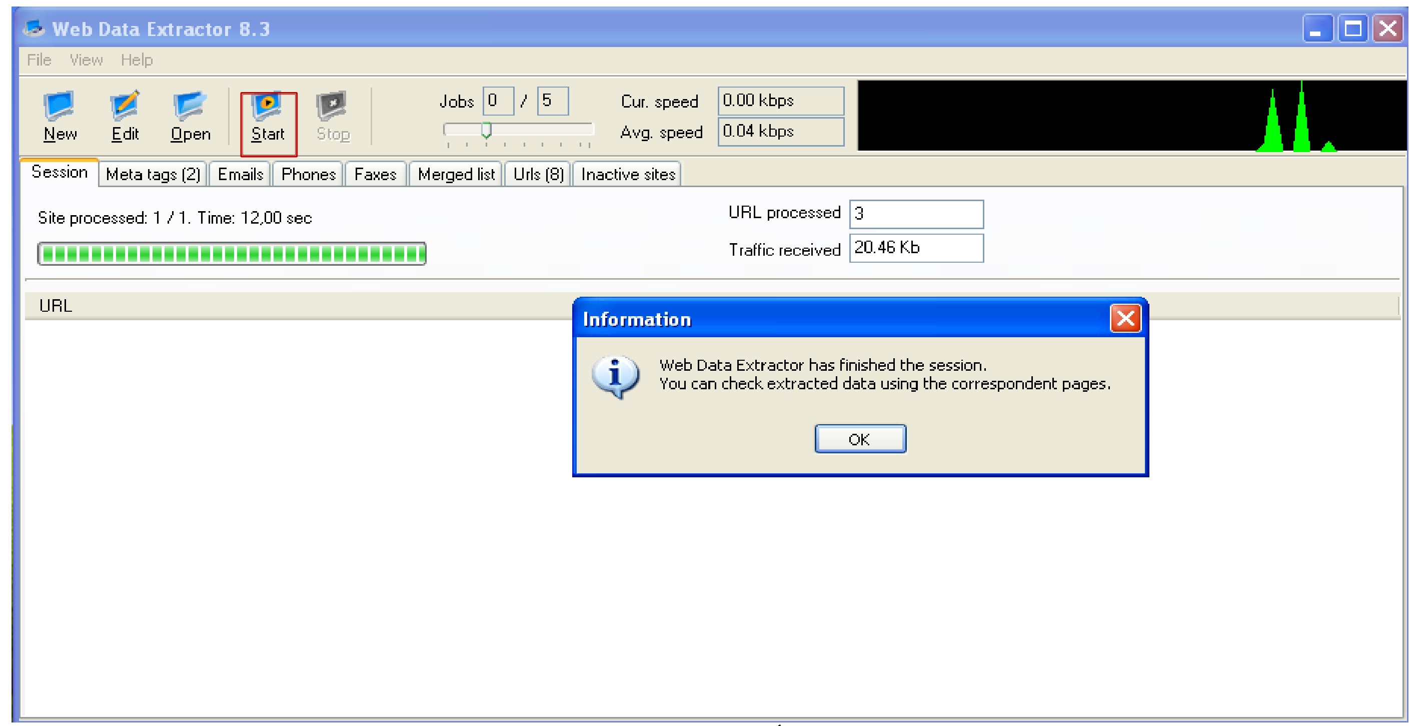
1- نقوم بتثبيت التطبيق باتباع الـ **wizard** الخاص بعملية التثبيت.
2- بعد الانتهاء من عملية التثبيت نقوم بتشغيل البرنامج من خلال الأيقونة المعبرة عنه فتظهر الشاشة التالية:



3- نضغط على الزر **New** لبدا **session** جديد فتظهر الشاشة التالية والتي نقوم فيها بإدخال عنوان **URL** عن المنظمة الهدف وليكن مثلا هنا **http://www.certifiedhacker.com** ثم عمل **CHECK BOXS** على جميع الخيارات المتاحة كالاتى:



4- ثم نضغط على **OK** فنرجع الى الشاشة الرئيسية ونضغط على **start** لنبدأ جمع المعلومات وعند الانتهاء يخبرك برسالة انه قد أنهي عملية جمع المعلومات كالاتى:



5- يمكن عرض نوعية المعلومات بالتنقل بين الازرار الأتية:



6- يمكن ايضا حفظ المعلومات التي قمت بجمعها عن طريق الضغط على **File** ثم **Save Session** ونحدد المكان الذي نحفظ فيه.

ADDITIONAL FOOTPRINTING TOOLS

بالإضافة الى الأدوات المستخدمة في عملية الاستطلاع التي تم ذكرها لاحقا هناك عدة أدوات أخرى كالاتي:

Prefix WhoIs available at **http://pwhois.org**
NetScanTools Pro available at **http://www.netscantools.com**
Tctrace available at **http://www.phenoelit-us.org**
Autonomous System Scanner (ASS) available at **http://www.phenoelit-us.org**
DNS DIGGER available at **http://www.dnsdigger.com**
Netmask available at **http://www.phenoelit-us.org**
Binging available at **http://www.blueinfy.com**
Spiderzilla available at **http://spiderzilla.mozdev.org**
Sam Spade available at **http://www.majorgeeks.com**
Robtex available at **http://www.robtex.com**
Dig Web Interface available at **http://www.digwebinterface.com**
Domain Research Tool available at **http://www.domainresearchtool.com**
Activewhois available at **http://www.johnru.com**
yoName available at **http://yoname.com**
Ping-Probe available at **http://www.ping-probe.com**
SpiderFoot available at **http://www.binarypool.com**
CallerlP available at **http://www.callerippro.com**
Zaba Search available at **http://www.zabasearch.com**
GeoTrace available at **http://www.nabber.org**
DomainHostingView available at **http://www.nirsoft.net**

(الحماية من عمليات الاستطلاع) FOOTPRINTING COUNTERMEASURES 2.5

حتى الآن ناقشنا أهمية **Footprinting**، ومختلف الطرق التي يمكن أن يؤديها **Footprinting**، والأدوات التي يمكن استخدامها لل **Footprinting**. الآن سوف نناقش المضادات ليتم تطبيقها من أجل تجنب الكشف عن المعلومات الحساسة.

Footprinting Countermeasures هي تدابير أو إجراءات متخذة لمواجهة أو تعويض الإفصاح عن المعلومات. وفيما يلي بعض التدابير المضادة لعملية الا **Footprinting** على النحو التالي:

1- إعداد أجهزة التوجيه [**router**]للحد من الرد على طلبات الا **Footprinting**.
2- قفل المنافذ مع تكوين جدار الحماية المناسب.
3- تقييم والحد من كمية المعلومات المتاحة قبل نشرها على موقع/شبكة الإنترنت وتعطيل الخدمات الغير ضرورية.
4- منع محركات البحث من التخزين المؤقت [**caching**]لل **webpage** واستخدام خدمات تسجيل المجهول.
5- إعداد خوادم الويب لتجنب تسرب المعلومات وتعطيل البروتوكولات غير المرغوب فيها.
6- استخدام **IDS** التي يمكن إعداده لرفض الحركات المشبوهة والتقاط أنماط **Footprinting**.
7- أداء تقنية الا **Footprinting** وإزالة أي معلومات حساسة يتم العثور عليها.
8- فرض السياسات الأمنية لتنظيم المعلومات التي من الممكن أن تكشف لأطراف ثالثة بواسطة الموظفين.
9- فصل مجموعة **DNS** الداخلية عن مجموعة **DNS** الخارجية.
10- تعطيل قوائم الدليل واستخدام **split-DNS**.
11- تثقيف الموظفين حول مختلف الحيل المستخدمة من قبل الهندسة الاجتماعية والمخاطر.
12- تقييد المدخلات غير متوقعة مثل **|؛ <>**.
13- تجنب domain-level وcross-linking للأصول الحرجة.
14- تشفير كلمات المرور وحماية المعلومات الحساسة.
15- عدم تمكين البروتوكولات التي ليست مطلوبة.
16- استخدام دائما **TCP / IP** و**IPsec**.
17- إعداد **IIS** ضد **banner gabbing**.

FOOTPRINTING PENETRATION TESTING 2.6

حتى الآن ناقشنا كل التقنيات والأدوات اللازمة لاختبار أمن النظام أو الشبكة اللازمة. الآن حان الوقت لوضع كل تلك التقنيات في وضع العمل. اختبار أمن النظام أو الشبكة باستخدام تقنيات مماثلة لتلك التي يستخدمها المهاجمين مع أذونات كافية يعرف باسم اختبار الاختراق. وينبغي إجراء اختبار الاختراق للتحقق ما إذا كان المهاجم قادرا على الكشف عن معلومات حساسة ردا على محاولات **Footprinting**. اختبار الاختراق [**Penetration testing**] هو وسيلة تقييم للنظام أو أمن الشبكة. في هذا الأسلوب من التقييم، يعمل مؤدى هذا النوع من الاختبار [**pen tester**] باعتباره شخص خارجي يريد اختراق النظام حيث يحاكي هجوما للقرصنة من اجل العثور على الثغرات الأمنية.

FOOTPRINTING PEN TESTING

Footprinting Pen Testing يستخدم لتحديد طبيعة معلومات المؤسسة المتاحة للجمهور على شبكة الإنترنت مثل هندسة الشبكات وأنظمة التشغيل والتطبيقات و المستخدمين. في هذه الطريقة، يحاول **Pen Tester** جمع المعلومات الحساسة المتاحة للجمهور عن الهدف من خلال التظاهر بانه مهاجم. قد يكون الهدف مجموعة محددة أو شبكة.

Pen tester يمكنه تنفيذ أي هجوم مثل ما يمكنه ان يؤديه المهاجم. **Pen tester** يجب عليه ان يحاول استخدام كل الطرق الممكنة لجمع أكبر قدر ممكن من المعلومات لضمان الحد الأقصى من نطاق الاختبار **Footprinting Pen Testing** . إذا وجد الـ **Pen tester** أية من المعلومات الحساسة موجودة على أي مورد من المعلومات المتاحة للجمهور، فانه يجب إدخال هذه المعلومات وكتابة تقرير عن ذلك.

أهم مزايا إجراء اختبار الاختراق Pen testing ما يلي:

- يوفر لك فرصة لمنع استرجاع سجل **DNS** من الخوادم المتاحة للعموم.
- يساعدك على تجنب تسرب المعلومات.
- يمنع محاولات الهندسة الاجتماعية.

اختبار الاختراق [Penetration test] هو وسيلة إجرائية لاختبار الأمن والمتمثل في الخطوات التالية المختلفة. ينبغي اتباع الخطوات التالية واحدة تلو الأخرى من أجل ضمان أقصى قدر من نطاق الاختبار. هنا هي الخطوات المتبعة في Footprinting Pen testing:

1- الخطوة الأولى: Get proper authorization (الحصول على الترخيص اللازم)

يجب أن يتم تنفيذ **Pen test** مع إذن. لذا، فإن الخطوة الأولى من **Footprinting pen testing** هو الحصول على الترخيص اللازم من الاشخاص المسئولين، مثل مسئولي النظام [**admin**].

2- الخطوة الثانية: Define the scope of the assessment (تحديد نطاق التقييم)

تحديد نطاق التقييم الأمني هو شرط مسبق لاختبار الاختراق. تحديد نطاق التقييم يحدد مجموعة من الأنظمة في الشبكة وذلك لفحصها والموارد التي يمكن استخدامها في الاختبار، وما إلى ذلك. يحدد أيضا حدود الـ **Pen tester**. بمجرد تحديد النطاق، يجب أن تخطط لجمع المعلومات الحساسة باستخدام تقنيات **Footprinting** المختلفة.

3- الخطوة الثالثة: Perform Footprinting through search engines (إجراء Footprinting عن طريق محركات البحث)

Footprinting عن محركات البحث مثل **جوجل**، **ياهو**، **Ask**، **Bing**، **Dogpile**، وما إلى ذلك. لجمع المعلومات حول المنظمة المستهدفة مثل تفاصيل الموظفين، صفحات تسجيل الدخول، وبوابات الإنترانت(**gateway**)، الخ. والتي يمكنها أن تساعدك في أداء الهندسة الاجتماعية وغيرها من أنواع متقدمة من الهجمات.

4- الخطوة الرابعة: Perform website Footprinting (أداء عملية الاستطلاع عن المواقع الإلكترونية)

أداء عملية الاستطلاع عن المواقع الإلكترونية باستخدام أدوات مثل **HTTrack Web Site Copier**، **BlackWidow**، **Webripper**، وما إلى ذلك لبناء خريطة تفصيلية لبنية الموقع والهندسة المعمارية.

5- الخطوة الخامسة: Perform email Footprinting (عملية الاستطلاع باستخدام البردي الإلكتروني)

أداء عملية الاستطلاع باستخدام البريد الإلكتروني عن طريق استخدام أدوات مثل **eMailTrackerPro**، **PoliteMail** ، **Email Lookup - Free Email Tracker** ، وما إلى ذلك. لجمع معلومات حول الموقع الفعلي للفرد لأداء الهندسة الاجتماعية والتي بدورها قد تساعد في رسم خرائط الشبكة للمنظمة الهدف.

6- الخطوة السادسة: Gather competitive intelligence (جمع معلومات عن المنافسين)

جمع المعلومات الاستخباراتية عن الشركات/المنظمات التنافسية باستخدام أدوات مثل **Hoovers**، **SEC Info**، **Business Wire**، وما الى ذلك. هذه الأدوات تساعدك على استخراج المعلومات حول المنافس مثل إنشائها وموقع الشركة، وتحليل تقدمها في السوق، السلطات العليا، وتحليل المنتج وتفاصيل التسويق، وأكثر من ذلك.

7- **الخطوة السابعة: Perform Google hacking (تنفيذ قرصنة جوجل)**

أداء قرصنة جوجل باستخدام أدوات مثل **GHDB**، **MetaGoofil**، **SiteDigger**، وما إلى ذلك. يحدد الثغرات الأمنية في الرمز الكودى واعداد المواقع. عادة ما يتم قرصنة جوجل بمساعدة مشغلي جوجل المتقدمة التي تحدد سلاسل محددة من النص مثل إصدارات تطبيقات الويب التي بها نقاط الضعف.

8- **الخطوة الثامنة: Perform WHOIS Footprinting (عملية الاستطلاع باستخدام قواعد whois)**

أداء تقنية **WHOIS Footprinting** لاستخراج معلومات حول دومين معين. يمكنك الحصول على معلومات مثل اسم الدومين وعنوان **IP**، اسم مالك الدومين، الاسم المسجل، وتفاصيل الاتصال بهم بما في ذلك أرقام الهاتف، البريد الإلكتروني، وما إلى ذلك. أدوات مثل **Smartwhois**، **Countrywhois**، **Whois Pro** و**Activewhois** تساعدك على استخراج هذه المعلومات. يمكنك استخدام هذه المعلومات لأداء الهندسة الاجتماعية للحصول على مزيد من المعلومات.

9- **الخطوة التاسعة: Perform DNS Footprinting (أداء عملية الاستطلاع عن قواعد DNS)**

أداء **DNS Footprinting** باستخدام أدوات مثل **DIG**، **NSLOOKUP**، **DNS record**، وما إلى ذلك. لتحديد المضيفين الرئيسين في الشبكة وأداء هجمات الهندسة الاجتماعية. حل اسم الدومين لمعرفة عنوان **IP** الخاص به، وسجلات **DNS**، وما الى ذلك.

10- **الخطوة العاشرة: Perform network Footprinting (أداء عملية الاستطلاع عن الشبكة)**

أداء **Network Footprinting** باستخدام أدوات مثل **Path Analyzer Pro**، **VisualRoute 2010**، **Network Pinger**، وما إلى ذلك. لإنشاء خريطة للشبكة الهدف. **Network Footprinting** يسمح لك للكشف عن نطاق الشبكة ومعلومات عن الشبكات الأخرى من الشبكة المستهدفة. باستخدام كل هذه المعلومات، يمكنك رسم "الرسم تخطيطي" للشبكة عن الشبكة الهدف.

11- **الخطوة الحادية عشر: Perform social engineering (تنفيذ الهندسة الاجتماعية)**

تنفيذ تقنيات الهندسة الاجتماعية مثل **eavesdropping** و**shoulder surfing** و**dumpster diving** التي قد تساعد على جمع المعلومات الأكثر أهمية عن المنظمة الهدف. من خلال استخدام الهندسة الاجتماعية فأنه يمكنك جمع تفاصيل عن الموظفين في المنظمة الهدف، وأرقام الهواتف، والعناوين، وعنوان البريد الإلكتروني، وما إلى ذلك. يمكنك استخدام هذه المعلومات لكشف المزيد من المعلومات.

12- **الخطوة الثانية عشر: Perform Footprinting through social networking sites (من خلال الشبكات الاجتماعية)**

أداء **Footprinting** من خلال مواقع التواصل الاجتماعي على موظفي المنظمة الهدف التي تم الحصول على أسمائهم من خلال عملية الهندسة الاجتماعية. يمكنك جمع المعلومات الشخصية من ملفاتهم الشخصية على مواقع الشبكات الاجتماعية مثل **الفاسبوك**، **LinkedIn**، **تويتر**، **جوجل+**، **Pinterest** وما الى ذلك، والتي تساعد في أداء الهندسة الاجتماعية. يمكنك أيضا استخدام الناس كمحركات بحث للحصول على معلومات حول الشخص الهدف.

13- **الخطوة الثالثة عشر: Document all the findings (توثيق جميع النتائج)**

بعد تنفيذ كل تقنيات الـ **Footprinting**، وجمع وتوثيق جميع المعلومات التي تم الحصول عليها في كل مرحلة من مراحل الاختبار. يمكنك استخدام هذه الوثيقة لدراسة وفهم وتحليل الوضع الأمني للمنظمة المستهدفة. هذا يتيح لك أيضا العثور على الثغرات الأمنية. عندما تجد الثغرات الأمنية، يجب أن تشير إلى التدابير المضادة لهذه الثغرات.

FOOTPRINTING PEN TESTING REPORT TEMPLATES (قالب/شكل تقارير عملية اختبار الاختراق)

عادة ما يتم إجراء اختبار الاختراق لتعزيز الأمن في محيط المؤسسة. بمثابة إنك **Pen Tester** فأنه يجب عليك جمع المعلومات الحساسة مثل تفاصيل الخادم، نظام التشغيل، وما إلى ذلك حول الهدف من خلال إجراء**Footprinting** . عملية تحليل النظام وشبكة الدفاعات عن طريق كسر أمنها مع أذونات كافية (أي أخلاقيا) دون التسبب في أي ضرر. العثور على الثغرات ونقاط الضعف في الشبكة أو أمن النظام. الآن شرح جميع نقاط الضعف جنبا إلى جنب مع التدابير المضادة المعنية في التقرير، مثل تقرير **Pent tester**. تقرير **Pent tester** هو تقرير حصلت بعد أداء اختبارات اختراق الشبكة أو تدقيق أمنى. فهو يحتوي على كل التفاصيل مثل نوع الاختبارات التي قمت بها، وأساليب القرصنة المستخدمة، ونتائج عملية القرصنة. بالإضافة إلى ذلك، يتضمن التقرير أيضا المخاطر الأمنية ونقاط الضعف للمؤسسة. إذا تم تحديد أي الضعف خلال أي اختبار، فانه يجب ذكر تفاصيل سبب الضعف جنبا إلى جنب مع التدابير المضادة. وينبغي دائما أن يبقى التقرير سري. إذا وقعت هذه المعلومات في أيدي المهاجمين فأنها قد تستخدم لشن هجمات.

ينبغي أن يتضمن تقرير الاختبار التفاصيل التالية:

Pen Testing Report

Information obtained through search engines	Information obtained through people search
Employee details:	Date of birth:
Login pages:	Contact details:
Intranet portals:	Email ID:
Technology platforms:	Photos:
Others:	Others:
Information obtained through website footprinting	**Information obtained through Google**
Operating environment:	Advisories and server vulnerabilities:
Filesystem structure:	Error messages that contain sensitive information:
Scripting platforms used:	Files containing passwords:
Contact details:	Pages containing network or vulnerability date:
CMS details:	Others:
Others:	
Information obtained through email footprinting	**Information obtained through competitive intelligence**
IP address:	Financial details:
GPS location:	Project plans:
Authentication system used by mail server:	Others:
Others:	



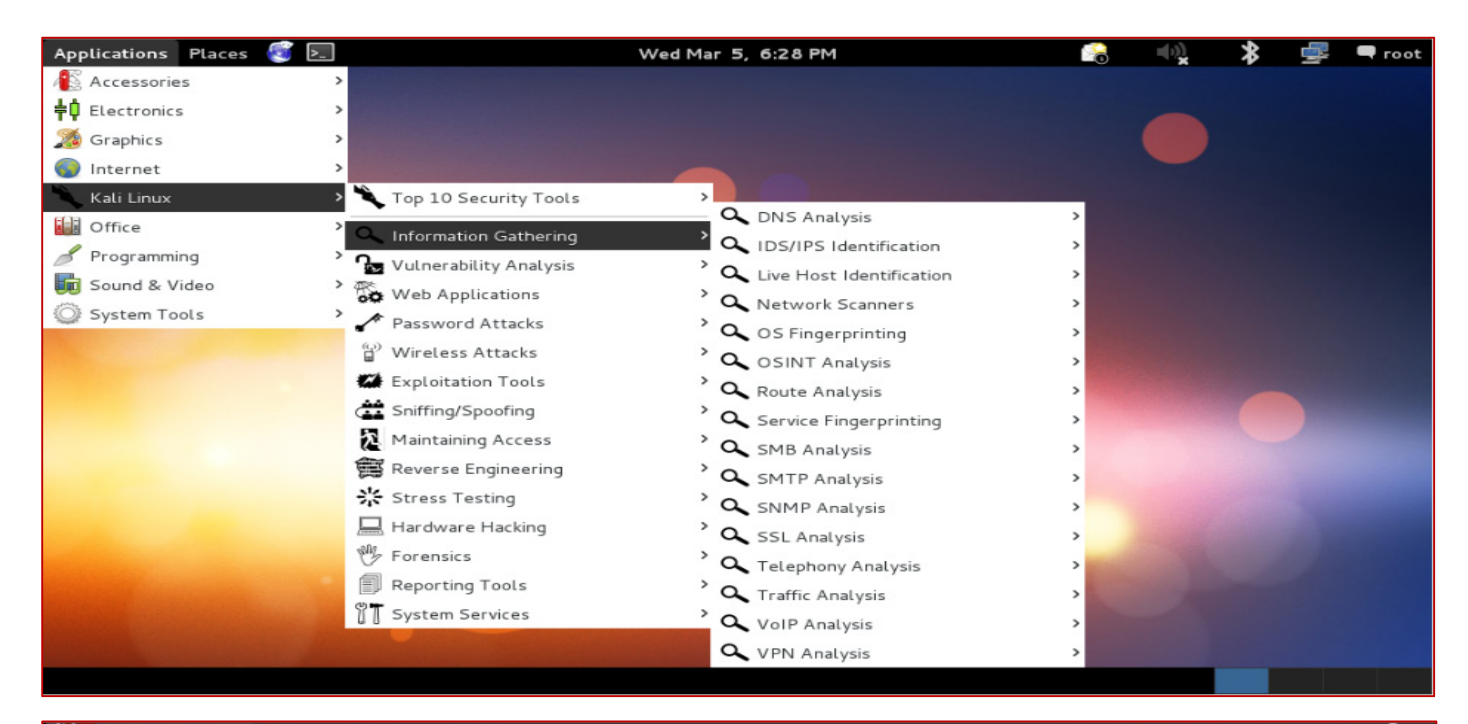
Pen Testing Report

Information obtained through WHOIS footprinting	Information obtained through social engineering
Domain name details:	Personal information:
Contact details of domain owner:	Financial information:
Domain name servers:	Operating environment:
Netrange:	User names and passwords:
When a domain has been created:	Network layout information:
Others:	IP addresses and names of servers:
Information obtained through DNS footprinting	Others:
Location of DNS servers:	
Type of servers:	
Others:	
Information obtained through network footprinting	**Information obtained through social networking sites**
Range of IP addresses:	Personal profiles:
Subnet mask used by the target organization:	Work related information:
OS's in use:	News and potential partners of the target company:
Firewall locations:	Educational and employment backgrounds:
Others:	Others:

OTHER TECHNIQUE OF INFORMATION GATHERING WITH KALI LINUX 2.7

ملحوظه: في هذا الجزء سوف نتكلم عن بعض الأدوات الأخرى المستخدمة في جمع المعلومات عن طريق استخدام نظام التشغيل جنو/لينكس "التوزيعة كالي لينكس وباك تراك 5".

تحتوي توزيعة كالي لينكس وباك تراك 5 على قائمه غنيه بالأدوات تحت عنوان **Information Gathering** مخصصه لعملية ال**Footprinting**. يمكن أن تملأ كتابا منفصلا لتغطية كافة الأدوات والأساليب المتاحة لجمع المعلومات. سيركز هذا الجزء على باقي مواضيع الاستطلاع الموجودة على الإنترنت، وتلك التي توفرها كالي لينكس.





COMPANY WEBSITE

هناك الكثير من المعلومات القيمة التي يمكن الحصول عليها عن موقع الويب المستهدف. أكثر مواقع الشركات تضع قائمه بفريقهم التنفيذي والشخصيات العامة، وأعضاء من التوظيف والموارد البشرية. يمكن أن تصبح هذه الأهداف عرضه لجهود البحث الأخرى وهجمات الهندسة الاجتماعية.

يمكن الحصول على معلومات أكثر قيمة من خلال النظر في الشركات الأخرى المدرجة كشركاء، الوظائف الخالية الحالية، المعلومات التجارية، والسياسات الأمنية. عملية الاستطلاع عن الشريك ذو المركز الاعلى يمكن أن يكون هاما مثل الهدف الرئيسي، وذلك لأن الشركاء قد يوفروا مصدرا جديدا للحصول على معلومات استخبارية.

الملف **robots.txt** متاح للعامة ويوجد في المواقع التي تعطي تعليمات **robots** على شبكة الإنترنت بمنع محركات البحث من الوصول الى الملفات المهمة (محركات البحث تعرف أيضا باسم محركات العناكب للبحث"**search engine spiders**")، وهذا يطلق عليه **The Robots Exclusion Protocol** .

التعبير "**Disallow : /**" يخبر المتصفح بعدم إمكانية زيارة المجلدات الرئيسية، ومع ذلك، يمكن تجاهلها بإعطاء الباحثين الاذكياء هدف لجعله يكون متاحا للعامة.

لعرض الملف **Robots.txt**، يجب العثور عليه في المسار الجذري للموقع الهدف. على سبيل المثال، نضيف التعبير"**robots.txt**" للموقع مثال كالاتى: " **http://www.facebook.com/robots.txt**"

```
Firefox    http://www.facebook.com/robots.txt
www.facebook.com/robots.txt

# Notice: Crawling Facebook is prohibited unless you have express written
# permission. See: http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: baiduspider
Disallow: /ajax/
Disallow: /album.php
Disallow: /autologin.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /l.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photos.php
Disallow: /sharer/

User-agent: Googlebot
Disallow: /ajax/
Disallow: /album.php
Disallow: /autologin.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /l.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photos.php
Disallow: /sharer/

User-agent: msnbot
Disallow: /ajax/
Disallow: /album.php
Disallow: /autologin.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /l.php
Disallow: /p.php
Disallow: /photo.php
```

THE HARVESTER: DISCOVERING AND LEVERAGING E-MAIL ADDRESSES

Harvester اداة ممتازة لاستخدامها في عمليات الاستطلاع. **Harvester** بسيط في عمله ولكنه سكريبت قوى وفعال من النوع بايثون كتبه كريستن مورتوريلا [**Christian Martorella**]. هذه الأداة تسمح لنا بسرعة وبدقة سرد كلا عناوين البريد الإلكتروني والنطاقات/الدومين الفرعية التي ترتبط مباشرة بهدفنا.

من المهم دائما استخدام أحدث نسخة من **Harvester** وذلك لان العديد من محركات البحث تعمل على تحديث وتغيير أنظمتها بانتظام. حتى التغيرات الطفيفة لسلوك محرك البحث يمكن أن تجعل الأدوات الآلية غير فعالة. في بعض الحالات، تقوم محركات البحث بتحديد النتائج قبل عودته المعلومات لك. أيضا العديد من محركات البحث تستخدم تقنيات [**throttling techniques**] من شأنها أن تحاول ان تمنعك من تشغيل عمليات البحث الآلي.

Harvester يمكن استخدامها للبحث في جوجل (**google**)، بنج(**Bing**) ، وخوادم الـ **PGP** لرسائل البريد الإلكتروني ، والمضيفين (**hosts**) ، والنطاقات الفرعية(**subdomain**) . يمكن أيضا البحث في **LinkedIn** عن أسماء المستخدمين. معظم الناس تعتبر تحميل عنوان البريد الإلكتروني الخاص بهم غير حميدة. لقد ناقشنا بالفعل مخاطر الإرسال إلى المنتديات العامة باستخدام عنوان البريد الإلكتروني الخاص بك المتوفر من قبل الشركة الخاصة بك، ولكن هناك مخاطر إضافية يجب أن تكون على علم بها. دعونا نفترض مثلا من خلال عملية الاستطلاع الخاص بك للكشف عن عناوين البريد الإلكتروني للموظفين الذين يعملون في المنظمة التي تستهدفها. قبل البحث ومعالجة المعلومات قبل الرمز " @ "، يجب أن نكون قادرين على إنشاء سلسلة من أسماء المستخدمين المحتملين للشبكة. ليس بالمألوف لدى المنظمات استخدام أسماء المستخدم وعناوين البريد الإلكتروني نفسهم (قبل الرمز "@"). مع حفنة من أسماء المستخدمين المحتملين، يمكننا محاولة جعل **brute force** يجد طريقه إلى أية خدمات، مثل **Secure Shell**، **Virtual Private Networks** (**VPN**)، أو بروتوكول نقل الملفات (**FTP**)، والتي سوف نكتشفها أثناء الخطوة 2 (**Scanning**).

Harvester هو اداه مبنيه داخل كالي. أسرع طريقة للوصول إلى **Harvester** هو فتح نافذة الترمنال وكتابة الأوامر **theharvester**. إذا كنت في حاجة إلى المسار الكامل للبرنامج وكنت تستخدم كالي، **Harvester** (وتقريبا كل الأدوات الأخرى) يمكن العثور عليها في المجلد **/usr/bin/**. مع ذلك، نذكر أن الميزة الرئيسية لكالي انه لم يعد نحتاج لتشغيل أي اداه الوصول الى المجلد الرئيسي الذي يحتوي على الأدوات مثل الباك تراك حيث إنك ببساطه تقوم بفتح الترمنال وكتابة الامر.

ملحوظه: إذا كنت تعمل على نظام تشغيل لينكس ولكن توزيع أخرى غير كالي او باك تراك فيمكنك تحميل هذه الأداة من الموقع التالي:

http://www.edge-security.com

مثل لتشغيلها في بك تراك بعد الذهاب الى المسار الخاص بها كالاتى:

$./theharvester.py©-d©syngress.com©-l©10©-b©google

مثل لتشغيلها في كالي

$theharvester©-d©syngress.com©-l©10©-b©google

```
root@jana:~# theharvester -d syngress.com -l 10 -b google

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|*
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|   *
*                                                                 *
* TheHarvester Ver. 2.2a                                          *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...

[+] Emails found:
------------------
solutions@syngress.com
chris@syngress.com
sales@syngress.com

[+] Hosts found in search engines:
------------------------------------
198.81.200.140:booksite.syngress.com
79.170.91.51:www.syngress.com
```

هذا الامر سوف يقوم بالبحث عن البريد الإلكتروني والنطاقات الفرعي[subdomain]والمضيفين[Hosts].

قبل مناقشة نتائج هذه الأداة، دعونا نبحث الأمر أقرب قليلا. يستخدم "**./theharvester.py او theharvester**" لاستدعاء الأداة. يستخدم التعبير [**-d**] لتحديد الدومين الهدف. يستخدم [**-l**] للحد من عدد النتائج التي يتم إرجاعها لنا. في هذه الحالة، فان هذه الأداة ترجع لنا 10 نتائج فقط. يتم استخدام [**-b**] لتحديد مستودع البحث الذي نريد ان نستخدمه. يمكننا الاختيار من بين مجموعة واسعة بما في ذلك **google**، **Bing**، **PGP**، **LinkedIn**، وأكثر من ذلك في هذا المثال، اخترنا البحث باستخدام جوجل. إذا لم تكن متأكدا من مصدر البيانات لاستخدامها في البحث الخاص بك، يمكنك أيضا استخدام [**-b all**] ليشمل جميع مستودعات البحث في وقت واحد للبحث والتي يمكن استخدامها.

الآن انت تفهم تماما كيفية استخدام الأمر لتشغيل الأداة، دعونا نلقي نظرة على النتائج. كما ترون، فان **harvester** فعال في تحديد العديد من عناوين البريد الإلكتروني التي يمكن أن تكون ذات قيمة بالنسبة لنا. هو أيضا ناجح في العثور على اثنين من النطاقات الفرعية. " **booksite.syngress.com** " و " **www.syngress.com** ".

METAGOOFIL

اداه أخرى ممتازة لجمع المعلومات وهي **MetaGoofil**. **MetaGoofil** هي أداة استخراج البيانات الوصفية (**metadata**) وتم كتابتها من قبل نفس الأشخاص الذين انشئوا **harvester**. غالبا ما تعرف البيانات الوصفية بأنها "بيانات عن البيانات". عند إنشاء مستند مثل **Microsoft Word** أو عرض تقديمي ل **PowerPoint**، يتم إنشاء بيانات إضافية وتخزينها داخل الملف. غالبا ما تشمل هذه البيانات قطعة مختلفة من المعلومات التي تصف الوثيقة بما في ذلك اسم الملف، حجم الملف، صاحب الملف أو اسم المستخدم الخاص بالشخص الذي قام بإنشاء الملف، والموقع أو المسار حيث تم حفظ الملف. تحدث هذه العملية تلقائيا دون أي تدخل او تفاعل من قبل المستخدم.

قدرة المهاجم على قراءة هذه المعلومات قد يقدم بعض الأفكار الفريدة عن المنظمة المستهدفة بما في ذلك أسماء المستخدمين، أسماء الكمبيوتر أو الخادم، مسارات الشبكة، الملفات المشاركة، وغيرها من الأشياء الجيدة. **MetaGoofil** هي الأداة التي تنظف الانترنت بحثا عن الوثائق التي تنتمي إلى الهدف الخاص بك. بعد العثور على هذه الوثائق، **MetaGoofil** يقوم بالتحميل لهم ومحاولا

استخراج البيانات الوصفية المفيدة. **MetaGoofil** بنيت في كالي ويمكن استخدامه من خلال فتح نافذة الترمنال و تشغيل الأمر "**metagoofil**"(جنبا إلى جنب مع رموز التبديل المناسبة) أو من خلال التنقل إلى مسار تنفيذ **MetaGoofil** الذي يقع في المجلد **/usr/bin.**

فكرة جيدة لإنشاء مجلد " ملفات ". الغرض من هذا المجلد هو حفظ كافة الملفات المستهدفة التي سيتم تحميلها، وهذا يحافظ على المجلد الأصلي نظيف.

يمكنك تشغيل **MetaGoofil** عن طريق إصدار الأمر التالي:

```
root@jana:~# ./metagoofil.py©-d syngress.com©-t©pdf,doc,xls,pptx©-n©20©-o©/files©-f©results.html
root@jana:~# metagoofil©-d©syngress.com©-t©pdf,doc,xls,pptx©-n©20©-o©/files©-f©results.html
```

```
root@jana:~# metagoofil -d syngress.com -t pdf,doc,xls,pptx -n 20 -o /files -f results.html

* Metagoofil Ver 2.2
* Christian Martorella
* Edge-Security.com
* cmartorella_at_edge-security.com

[-] Starting online search...
root@jana:~#
```

دعونا نبحث في تفاصيل هذا الأمر. يستخدم **metagoofil** لاستدعاء البرنامج النصي **MetaGoofil**. يتم استخدام [**-d**] لتحديد الدومين الهدف المراد تفتيشه. يتم استخدام [**-t**] التبديل لتحديد أي نوع أو أنواع الملفات التي تريد من **MetaGoofil** محاولة ايجاده وتحميله.

في وقت كتابة هذا التقرير، كان **MetaGoofil** قادرة على استخراج البيانات الوصفية من الصيغ التالية: **pdf، doc وxls وppt وodp، odx، docx، xlsx، pptx**. يمكنك إدخال أنواع ملفات متعددة عن طريق فصل كل نوع باستخدام الفاصلة (ولكن بدون مسافات). يتم استخدام [**-n**] لتحديد عدد الملفات من كل نوع التي ترغب في تحميله لفحصها. يمكنك أيضا تحديد أنواع الملفات الفردية للحد من النتائج التي تم إرجاعها. نستخدم التبديل [**-o**] لتحديد المجلد حيث نريد تخزين كل الملفات التي يقوم **MetaGoofil** بتحميله. أخيرا نستخدم التبديل [**-f**] لتحديد ملف الإخراج. هذا الأمر ينشا وثيقة تنسيق سهلة للمراجعة والفهرسة. افتراضيا سوف **MetaGoofil** أيضا عرض أية نتائج في الترمنال.

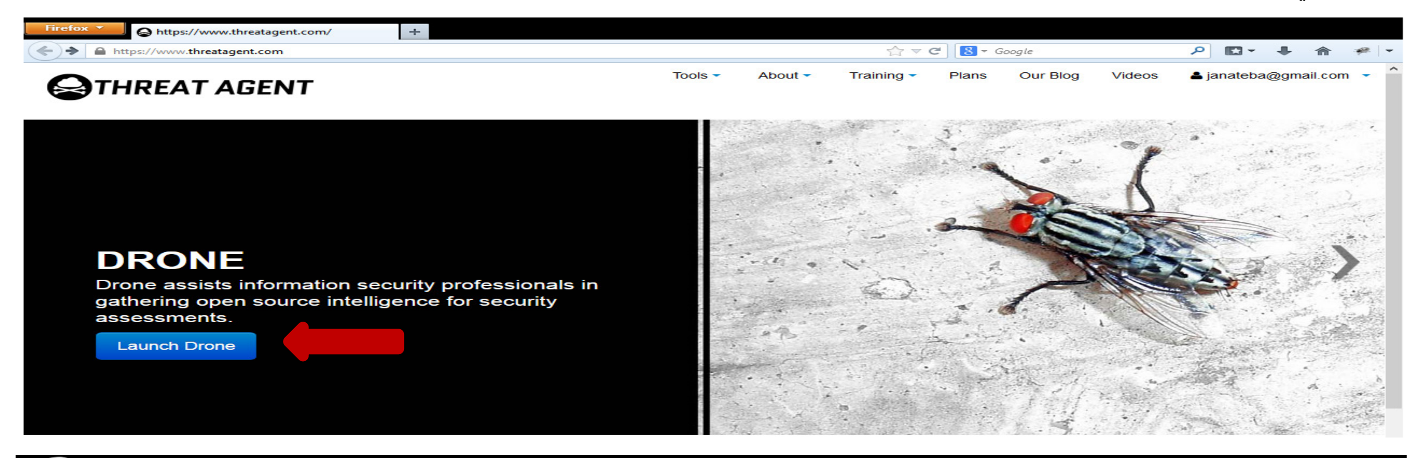
يوجد اداه شبيه بهذه الأداة وهيا goofile ويستخدم معها التعبيرين [-d] لتحديد الدومين الهدف و [-f] لتحديد نوع الملفات فقط

THREAT AGENT: ATTACK OF THE DRONES

خيار آخر للاستطلاع، والذي يتضمن العديد من أدوات لجمع المعلومات في مكان واحد، **ThreatAgent Drones**. وقد تم تطوير هذه الأداة من قبل ماركوس كاري. يمكنك التسجيل للحصول على حساب مجاني من خلال موقع الويب التالي:

https://www.threatagent.com

ThreatAgent يأخذك في جمع (**open source intelligence**) **OSINT** إلى المستوى التالي من خلال استخدام عدد من المواقع المختلفة، والأدوات، والتقنيات لإنشاء ملف كامل لك عن الهدف الخاص بك. الشيء الوحيد الذي تحتاجه هو اسم المؤسسة واسم النطاق كما هو مبين في الشكل.



DRONE

Open Source Intelligence

Deploy Drone

ثم نضغط هنا فتظهر شاشه
أخرى نضع بها اسم الدومين

Company Domain

New Drone Mission

Company Name:
google

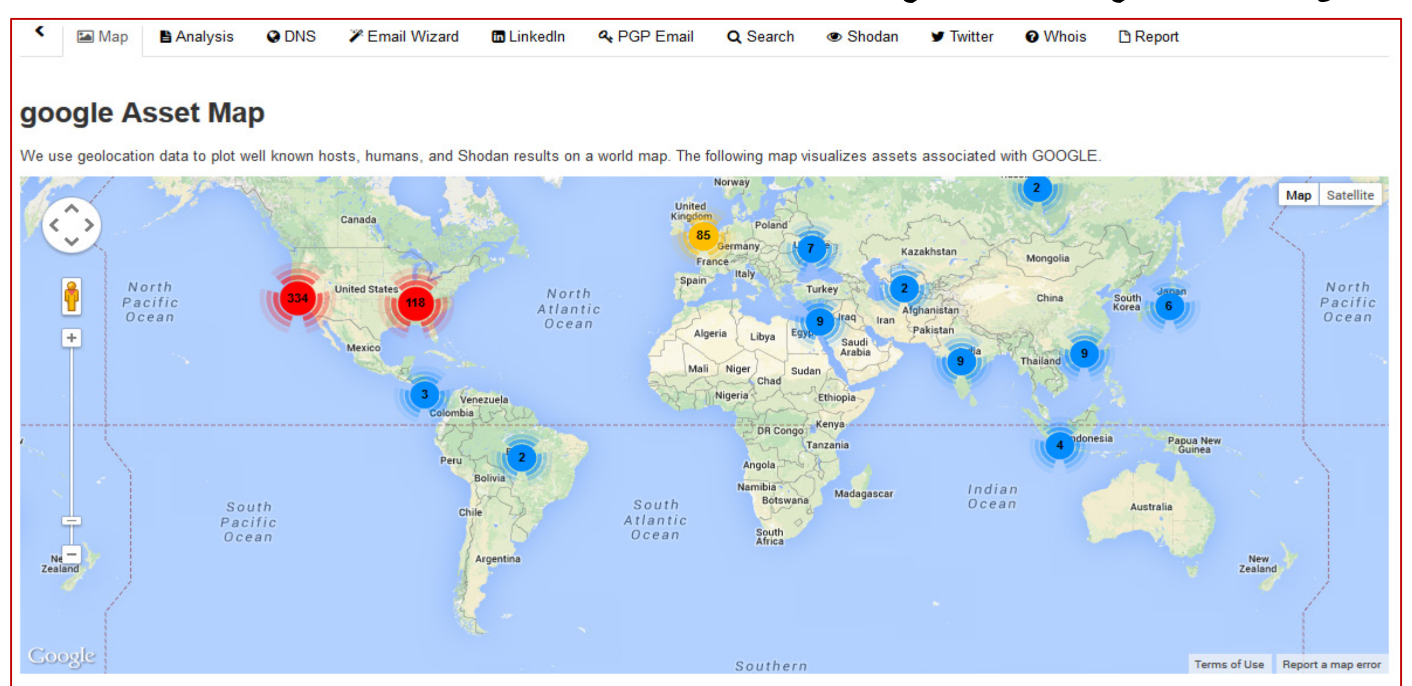
Domain Name:
google.com

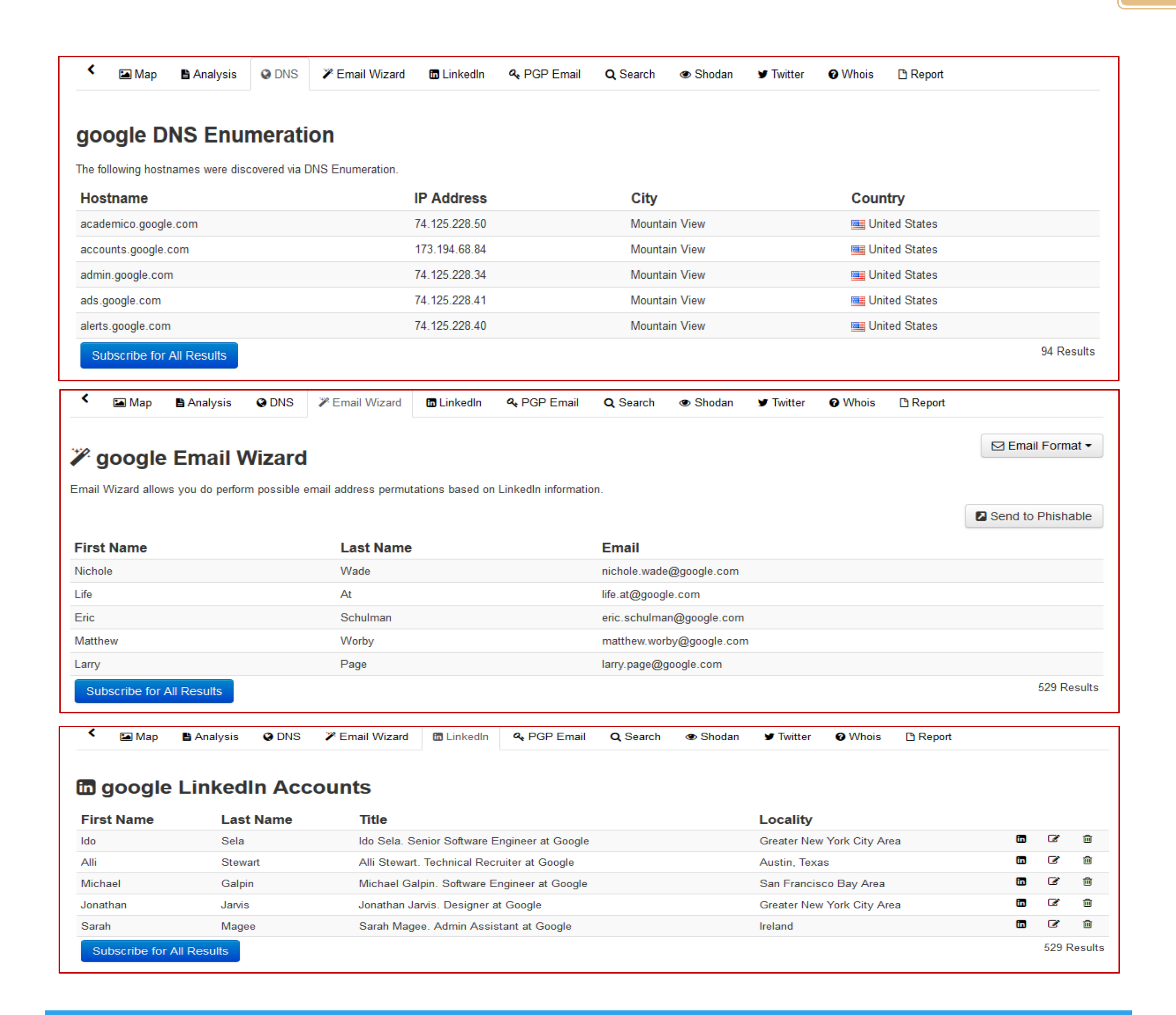
Deploy Drone

Company Domain

بمجرد انتهاء **Drone** من استخراج جميع المعلومات عن مختلف المواقع، فانه سوف يقدم تقريرا لك بعد ذلك عن نطاقات عناوين IP، وعناوين البريد الإلكتروني، وجهات الاتصال داخل المنظمة، والمنافذ (**ports**) المفتوحة [من خلال**Shodan**] ، وأكثر من ذلك بكثير. مثيرة للاهتمام بما فيه الكفاية.

انظر الى ما توصل اليه موقع الويب هذا من نتائج.





Hostname	IP Address	City	Country
academico.google.com	74.125.228.50	Mountain View	United States
accounts.google.com	173.194.68.84	Mountain View	United States
admin.google.com	74.125.228.34	Mountain View	United States
ads.google.com	74.125.228.41	Mountain View	United States
alerts.google.com	74.125.228.40	Mountain View	United States

First Name	Last Name	Email
Nichole	Wade	nichole.wade@google.com
Life	At	life.at@google.com
Eric	Schulman	eric.schulman@google.com
Matthew	Worby	matthew.worby@google.com
Larry	Page	larry.page@google.com

First Name	Last Name	Title	Locality
Ido	Sela	Ido Sela. Senior Software Engineer at Google	Greater New York City Area
Alli	Stewart	Alli Stewart. Technical Recruiter at Google	Austin, Texas
Michael	Galpin	Michael Galpin. Software Engineer at Google	San Francisco Bay Area
Jonathan	Jarvis	Jonathan Jarvis. Designer at Google	Greater New York City Area
Sarah	Magee	Sarah Magee. Admin Assistant at Google	Ireland

DARKNET، INVISIBLE WEB، HIDDEN WEB،DEEP WEB 2.8

- **مقدمه:**

لقد تم إدخال مصطلح "**deep web**" على مدى السنوات القليلة الماضية للدلالة على محتوى الإنترنت الذي لا يصل اليه محركات البحث. او بمعنى اخر هي جميع المحتويات الموجودة على شبكة الانترنت التي لا يمكن الوصول إليها مباشرة من خلال الارتباطات التشعبية [**hyperlinks**]. على وجه الخصوص: نماذج **HTML**، خدمات ويب. وهذه تمثل 500 مره أكثر من المحتوى على الشبكة العامة بالنسبة لإحصائية 2001 وهي تحتوي على مئات الآلاف من قواعد بيانات **deep web** على حسب احصائيات **2004**.

لا شك اننا جميعنا نستخدم الانترنت. لكن هل تعلم ان ما تتصفحه من على الانترنت العادي ليس كل محتوي الانترنت فهناك العديد من المواقع توجد ولا أحد يعلم عنها شيء. هذه الموقع وكل ما هو على شاكلتها من المواقع تقدم خدمات معينة يعلمها معظم مستخدمي الانترنت حول العالم. لكن ما لا تعلمه ان هناك العديم والعديد من المواقع التي لا يعلم عنها معظم مستخدمي الانترنت وهذه المواقع التي لا يعلم عنها معظم مستخدمي الانترنت تمثل اغلب محتوى الانترنت.

محتوى DEEP WEB كالاتى:

- **صفحات الويب الديناميكية** [Dynamic web pages]: الصفحات المولدة ديناميكيا من قبل HTTP (الانترنت العادي)
- **المواقع المحجوبة**[Blocked sites] : المواقع التي تحظر صراحة محركات البحث العنكبوتية مثل جوجل للذهاب واسترجاع محتوياتها عن طريق استخدام CAPTCHAs ، pragma no-cache HTTP headers، أو إدخالات ملف robots.txt ، على سبيل المثال.
- **المواقع غير مرتبطة**[Unlinked sites] : الصفحات التي لا ترتبط بأي صفحة أخرى، وتمنع محركات البحث العنكبوتية [Web crawler] من احتمالية الوصول إليها.
- **المواقع الخاصة**[private site] : الصفحات التي تتطلب التسجيل والتوثيق log-in/password للدخول اليها.
- **المواقع الغير** Non-HTML/Contextual/Scripted: المحتوى مشفرة في شكل مختلف، ويتم الوصول إليها عن طريق الجافا سكريبت أو فلاش، أو هي سياق معتمد (نطاق IP محدد).
- **شبكات محدودة الوصول**[Limited-access networks] : المحتوى على هذه المواقع لا يمكن الوصول إليها من قبل جمهور الانترنت العامة.

هاذين النقطتين تشكلا فئتين مستقلتين للDNS:

- Sites with domain names registered: مواقع ذات أسماء نطاقات مسجلة في خادم الاسماء (DNS) الجذري (أي نطاقات TLD). هذه هي المواقع التي تم تسجيلها باستخدام تقنية التسجيل المستقلة من قبل هيئة الإنترنت للأسماء والأرقام (ICANN) لتعيين أسماء المضيفين.

ICANN = Internet Corporation for Assigned Names and Numbers

أسماء النطاقات الافتراضية تتبع تسلسل هرمي في تسميتها والتي يتم تنسيقها من قبل ICANN، وهي المسؤولة عن تحديد نطاقات TLD القياسية (على سبيل المثال، com، edu، gov، وهكذا). بالتالي، تتم مزامنة DNSs القياسية وفقا لاسم التسلسل الهرمي الذي تم تعريفه من قبل ICANN ويمكنه ايضا حل جميع أسماء النطاقات المسجلة من قبل ICANN.

مع ذلك يمكن للمرء، الاتصال إلى ملقمات DNS الخاصة التي تدير مساحات إضافية غير معترف بها من قبل ICANN، مما يسمح بتسجيل أسماء نطاقات ولكنها لا تتبع قواعد ICANN مثل TLD الغير قياسي. في حين حل أسماء النطاقات هذه يتطلب استخدام خوادم DNS محددة، ويمكن استخدامها في تقديم بعض المزايا في شكل، وسيلة سهله لا يمكن تعقبها، وأحيانا لتسجيل أسماء النطاقات الجديدة.

- Darknet and alternative routing infrastructures: هي مواقع تم استضافتها على البنية التحتية التي تتطلب برامج محددة للوصول إلي محتوياتها. من أمثلة هذه النظم هي خدمات تور[TOR's] الغير مرئية أو المواقع المستضيفة على مشروع الإنترنت (I2P). يتم تحديد هذه المواقع بشكل عام وكذلك عن طريق اسم نطاق غير قياسي يتطلب استخدام نفس البرنامج لحلها إلى نقطة النهاية للتوجيه.

الجدير بالذكر أن محركات البحث العنكبوتية لا ترى مثل هذه المواقع، وذلك ليس بسبب وجود قيود التقنية. حيث يمكن لمواقع البحث العنكبوتية حل اسم DNS البديل من خلال ربطه إلى واحد من خوادم DNS المحددة والمتاحة للجمهور وتطبيقات TOR وI2P ويعمل وكأنه SOCKS proxy، مما يجعل من الممكن لمحركات البحث العنكبوتية للوصول إلى المحتويات المذكورة. حيث نلاحظ وجود تسرب ملحوظ وحيد للمعلومات من Darknet إلى محرك البحث وهذا يحدث بفضل خدمة gateway مثل tor2web، والذي يقدم نطاق/دومين للوصول إلى محتوى مواقع الخدمات المخفية مباشرة.

:TOR2WEB

المصدر: http://www.tor2web.org/config

هو عباره عن بروكسي يتم ربطه بمحركات البحث العنكبوتية مثل جوجل ليمكنه من البحث في مواقع الويب المخفية (deep web) ويمكنك معرفة طريقة فعل ذلك عن طريق الانتقال الى هذه الموقع ورؤية طريقة الربط.

يتم ذلك عن طريق استبدال الامتداد [.onion] بالامتداد [.tor2web.org] في المتصفح العادي بدون استخدام تطبيق خاص. لكن هذا لن يغنى عن استخدام التطبيق الخاص بهذه البيئة من الانترنت.

مثال على ذلك https://xzzpowtjlobho6kd.onion **فيصبح هكذا** https://xzzpowtjlobho6kd.tor2web.org

نظرة عامة على شبكات الإنترنت الموجودة في الخفاء (DEEP WEB)

حتى الآن، يوجد ثلاث شبكات رئيسية لمنح الاتصال الغير مرئي لكل من العميل والخادم هما **TOR**، **I2P**، و**Freenet**.

ملحوظه: الاثنين الاخرين لم يصلا بعد إلى نفس الاعتماد الذي وصلت إليه TOR ولكن الميزات التقنية الحالية التي يملكونها يمكن أن تؤدي إلى أن يصبحوا بدائل قابلة للتطبيق في المستقبل القريب (على سبيل المثال، تصبح شبكة TOR لا يمكن الاعتماد عليها للغاية بالنسبة للمستخدمين).

شبكة TOR

وضعت شبكة **TOR** في الأصل من قبل مختبر أبحاث للبحرية الأمريكية [**U.S. Naval Research Laboratory**]. قدم للمرة الأولى في عام 2002. فإنه يسمح للاتصالات المجهولة من خلال استغلال شبكة من **volunteer nodes** (أي أكثر من 3،000 حتى الآن) المسؤولة عن توجيه طلبات مشفرة بحيث يمكن إخفاء حركة مرور البيانات من أدوات مراقبة الشبكة.
للاستفادة من شبكة **TOR**، يحتاج المستخدم لتثبيت البرامج التي تعمل بمثابة **SOCKS proxy**. برنامج **TOR** يخفي الاتصالات إلى أي خادم/سيرفر على شبكة الإنترنت عن طريق اختيار عدد من العقد (**node**)ذات تتابع العشوائي لتشكيل دائرة. قبل الدخول إلى الشبكة، يتم تشفير كل طلب بشكل متكرر باستخدام المفتاح العمومي لكل عقدة محددة. ثم، من خلال الارتداد من تتابع[**relay**] واحدة إلى أخرى، ورفع كل طبقة من التشفير قبالة التتابع التالي، حتى يتم الوصل إلى عقدة الخروج ومن ثم يمكن للطلب الغير مشفر الذهاب إلى وجهتها.

اعتماد هذه الآلية من التشفير متعدد الطبقات يعطي المزايا التالية:

- الخادم/الملقم الذي يتلقى الطلب القادم من شبكة **TOR** سوف ترى بأنها صادرة عن العقدة الأخيرة في دائرة **TOR** (أي عقدة الخروج[**exit node**]) ولكن هناك توجد طريقة واضحة لتتبع طلب العودة إلى أصله.
- كل عقدة [**node**] داخل الدائرة لا تعرف سوى **hop** السابق والتالي للطلب ولكنه لا يمكن فك محتوياته ولا معرفة وجهتها النهائية.
- العقدة الوحيدة التي يمكن **TOR** عرض طلب غير مشفرة هي عقدة الخروج ولكن حتى هذا لا يعرف أصل الطلب، يعرف فقط **hop** السابقة في الدائرة.

في الإصدارات الأخيرة من بروتوكول **TOR**، لقد تم إدخال وظائف جديدة للسماح لكامل المواقع ان يتم استضافتها على عقد **TOR**، مما يجعلها لا يمكن تعقبها. من المعروف أن الخدمات التي يتم تشغيلها ضمن شبكة **TOR** بأنها "خدمات خفية". **Approach** يعمل عن طريق تخزينه لمعلومات اتصال الوصول للخدمة الخفية على شكل عقدة الالتقاء (**rendezvous node**) التي سوف تعمل كوسيط وكمفتاح التشفير في [**Distributed Hash Table** (**DHT**)].
حيث يعتبر **DHT** بمثابة شكل من أشكال موزعي **DNS**، حيث تعمل على حل اسم المضيف **onion** إلى معلومات الاتصال اللازمة لتأسيس اتصال إلى الخدمة المخفية. في هذه الحالة، يتم أخفاء عناوين الـ **IP** لكل من العميل والملقم/الخادم من أي طرف ثالث يحاول تحليل أو منع حركة المرور. حتى يتم اخفاء المواقع الحقيقية عن بعضها البعض.
يمكن تحميل التطبيق المسئول عن الدخول الى شبكة TOR وهو متصفح تور من الرابط التالي:

https://www.torproject.org/

شبكة I2P

لقد تم تصميم **I2P** باعتباره [**anonymous peer-to-peer** (**P2P**)] تعمل على توزيع طبقة الاتصال والتي يمكنها تشغيل أي خدمة إنترنت تقليدية. قد تم تطويرها منذ عام 2003 باعتبارها تطوير لشبكة فرينيت[**Freenet network**] ، والذي يهدف الى السماح لعدة خدمات للتشغيل بجانب **HTTP**. بينما **TOR** انشاء في البداية لتمكين عدم الكشف عن الهوية عند الاتصال إلى خدمة الإنترنت (أي **WWW**) ثم مدد في وقت لاحق إلى الخدمات العامة الخفية، الهدف من **I2P** هو توفير وسيلة للمستخدمين للوصول الى الخدمات (على سبيل المثال، **IRC**، **web**، **mail** و**bit torrent**) بطريقة خفيه.
مشروع **I2P** اختصارًا لـ **Invisible Internet Project** هو برنامج حر ومجاني يمكن مستخدميه من الاتصال بدون الكشف عن الهوية على شبكة الإنترنت. الشبكة تمكن التطبيقات التي تستخدمها من الحفاظ على خصوصية المستخدم حيث تشمل تطبيقات التصفح المجهول، والدردشة، البريد الإلكتروني والمدونات ومشاركة الملفات. يهدف البرنامج إلى دعم حرية التعبير والرأي وتجاوز حجب المواقع على الأنترنت يمكنك التعبير عن رأيك بحرية دون الخوف من أن تعرف مستخدم البرنامج.

هي شبكة تخفي تؤمن طبقة يمكن أن تستخدمها التطبيقات الحساسة بالنسبة للهوية الشخصية للاتصال بشكل آمن حيث تغطى جميع البيانات بعدة مستويات من التشفير إضافةً لكون الشبكة موزعة وديناميكية بنفس الوقت بدون الاعتماد على أطراف موثوقة.
تتوافر العديد من التطبيقات التي تتخاطب مع **I2P** وتشمل البريد الإلكتروني، تطبيقات الندّ للندّ(**P2P**)، محادثة **IRC** وغيرها.

تمّ البدء بمشروع **I2P** في العام 2003 لدعم جهود كل من يحاول بناء المجتمع الحرّ وذلك من خلال تأمين نظام تواصل خفيّ، غير قابل للمراقبة وآمن **I2P**. هي نتاج جهود تضافرت لإنتاج شبكة قليلة التأخير ،موزعة بشكل كامل ،مستقلة ،خفيّة ،مرنة وآمنة. الهدف هو العمل بنجاح ضمن بيئة معادية بالرغم من كون موارد المنظمة المالية أو السياسية تحت الهجوم. كل ما يتعلق بهذه الشبكة مفتوح المصدر ومتوفر بدون أي تكلفة وهذا ما يضمن لمن يستخدمه أن هذه الشبكة تؤدي ما تدعيه، بالإضافة إلى تمكين الآخرين من المشاركة في تطويرها في مواجهة المحاولات العدوانية لخنق الكلمة الحرة.

التخفي ليس شيئاً حديّاً، بمعنى أننا لا نحاول أن نصنع شيئاً "خفياً بالكامل"، ولكن نعمل على أن نجعل الهجمات أكثر وأكثر تكلفةً لمن يريد أن يشنها. **I2P** هي مزيج من الشبكات قليلة التأخير وهناك حدود للتخفي الموفر بواسطة نظام كهذا، ولكن تطبيقات مثل **Syndie** ، **I2P mail**و**I2PSnark** توسع هذا النظام وتوفر المزيد من الوظائف الاضافية والحماية.
ما تزال **I2P** عملاً قيد الإنجاز لا يجب أن يعتمد عليه في الوقت الراهن في التخفي بشكل "مضمون" وذلك بسبب حجم الشبكة الصغير نسبياً وقلة المراجعة الأكاديمية المتوسعة. كما لا تعتبر حالياً منيعةً ضد الهجمات من قبل أشخاص بموارد غير محدودة وقد لا تكون أبداً كذلك، تبعاً للحدوديات الموروثة من كونها مزيج من الشبكات قليلة التأخير.

المبدأ الرئيسي لـ **TOR** هو خلق دوائر (أي مسارات مشفرة من خلال مجموعة عشوائية من العقد للوصول إما لعقدة الخروج التي هي بمثابة وكيل أو إلى نقطة الالتقاء التي تعمل كوسيط للتواصل مع خدمة الخفية). **I2P**، من ناحية أخرى، يستخدم الانفاق **TUNNEL**. كل عقدة في شبكة **I2P** هو جهاز التوجيه. أنه يخلق ويحافظ على مجموعة من المسارات الظاهرية الواردة والصادرة. على سبيل المثال، إذا عقدة **A** يريد أن يرسل رسالة إلى عقدة **B**، فإنه يقوم بتوجيه رسالة إلى واحدة من الأنفاق في الخارج جنبا إلى جنب مع المعلومات اللازمة للوصول إلى واحدة من الأنفاق الواردة.
يتم تخزين المعلومات حول الأنفاق الواردة، والتي تشبه إلى حد كبير في**TOR** ، في **DHT** التي هي بمثابة قاعدة بيانات شبكة لا مركزية.
يتم تشفير كل الاتصالات باستخدام طبقات متعددة: التشفير من نقطة إلى نقطة بين المرسل والمتلقي، والتشفير النقل بين أجهزة التوجيه في الشبكة، والتشفير من النهاية إلى النهاية في الأنفاق. نلاحظ أن، **TOR** يستخدم نظام تشفير يسمى "**onion routing**"، والتوجيه المشفر المستخدم في **I2P** يعرف باسم "**garlic routing**" والمواقع الخفية التي يتم استضافتها في شبكة **I2P**، تسمى أيضا "**eepsites**"
يمكنك تحميل التطبيق المسئول عن الولوج لهذه الشبكة من خلال الرابط التالي:

http://geti2p.net/en/

شبكة FREENET

Freenet تم تطويره منذ عام 2000، ويمكن اعتباره سلف لـ **I2P**. ولكنه على عكس **I2P**، حيث يقوم بتنفيذ **pure DHT** في شكل شبكة تراكب غير منظمه. هذا يعني أن كل عقدة مسؤولة عن مجموعة فرعية من الموارد المتاحة في الشبكة، ويقدم لهم التعاون عندما يتلقى الطلب. وعلاوة على ذلك، فان العقد تحفظ قائمة بالعقد المجاورة، والمعروفة عادة بالجيران الموثوقين، وذلك لزيادة الأمان. ويعرف هذا باسم "**small world principle**". العقد والبيانات يتم تعرفيهم بواسطة المفتاح، الممثلة عادة مع قيمة الهاش. عندما تبحث عن مورد ما، فان طلبك سوف يسافر عبر جميع العقد الجيران حسب الأفضلية.
فرينيت هو أكثر ملاءمة عند استخدام مع المحتوى الثابت مثل المواقع الثابتة ولا يتعامل بشكل جيد مع صفحات الويب المولدة ديناميكيا **HTTP** أو غيرها من أشكال خدمات الإنترنت (على سبيل المثال، IRC، والبريد، وغيرها).

ALTERNATIVE DOMAIN ROOTS

Alternative Domain Roots، المعروف أيضا باسم "**rogue TLDs**"، تشير إلى فئة من الشبكات التي تستخدم كيانات **DNS** ولكن التي ليست تحت سيطرة **ICANN**، وتكون على النقيض من النطاقات [**.com /.net /.org**] التقليدية. النطاقات المسجلة ضمن **rouge TLD** تتطلب استخدام خوادم أسماء (**named server**) مخصصه. من ناحية أخرى، اعتمادا على المؤسسة التي تعمل على تشغيل **DNS root**، فان تسجيل اسم الدومين قد يكون أقل إثارة للمشاكل لـ **malicious actors**، كما في حالة[**.bit domain**] ، لتسجيل نطاق جديد تتبع نموذج **P2P**. باختصار، هذا يعني أنه عند تسجيل اسم نطاق جديد فبدلا من التعامل مع السلطات المركزية يتم نشره مستقلا في شبكة **P2P** المصنوعة من كافة ملقمات [**.bit DNS**]. حتى يصبح كل ملقم/خادم على علم بالنطاقات المسجلة حديثا.

في حين ان **alternative DNS domains** لا يقدم أشكال معينة من عدم الكشف عن الهوية على عكس **TOR**، ولكنها تعرض بعض المزايا الواضحة لجهات **malicious actors**، مثل الحماية ضد **domain sinkholing** ومرونة في اداره الناطقات/الدومين، وحتى الآن، إمكانية "الهروب" من محرك البحث العنكبوتية. في حين انه من الممكن من الناحية الفنية لمحرك البحث العنكبوتي الوصول الى **alternative DNS domains** (على سبيل المثال، وذلك ببساطة باستخدام خوادم DNS الخاصة به)، فإنه لا يحدث عادة، وإذا كان كذلك، فلن تظهر النتائج للمستخدمين.

فيما يلي قائمه بـ**ALTERNATIVE DOMAIN ROOTS** الفعالة:

- **Namecoin**: مسؤول عن[**.bit TLD**] . هو قائم في عمله على **P2P** يعمل بنفس مبدأ **bitcoins**. للوصول إلى هذا الدومين من قبل العميل فانه يحتاج الى تشغيل **dedicated DNS client** أو الرجوع إلى أحد خوادم **DNS** التي تعتبر بوابة لهذه الشبكة على الإنترنت.
  يمكنك استخدام البلجن**FreeSpeechMe** على متصفح الفايرفوكس لرؤية المواقع [**.bit**] وذلك عن طريق الذهاب الى الموقع التالي [**http://www.freespeechme.org**] وهو أيضا يحتوى على قائمه بمواقع [**.bit**].
- **Cesidian root**: عباره عن **alternative DNS** تدار من قبل المواطنين الايطاليين تستخدم نطاقات **TLD** التالية [**.cw**], [**.ispsp**], [**.5w**], [**.6w**]. ولدت لتدعم رؤية **Mr. Tallini's** السياسية والذي يشغل أيضا منصب محافظ (**UMMOA**) وتعني **United Micronations Multioceanic Arcipelago** وهذا يضم 30 ملقم/خادم **DNS** حول العالم يعمل على كل من IPv4 وIPv6. لمزيد من المعلومات **http://cesidianroot.net**
- **Namespace.us**: هذه المنظمة تقدم 482 **Alternative TLD** مثل [**.academy - .big - .manifesto**]. وجدت في السوق منذ عام 1986، تأسست لتوسيع عدد محدود (في ذلك الوقت) من نطاقات **Alternative TLD** المتاحة، وقدمت أسرع عملية في تسجيل هذه النطاقات، فضلا عن الخدمات الأخرى ذات الصلة بالمجال. بعد أن فشلت في أواخر 1990 أن يكون لها نطاقات **TLD** متكاملة في منطقة **DNS root**، فإنه لا يزال موفر بديل لأسماء النطاقات حتى الآن، وتقدم خوادمها **DNS** الخاصة التي تعمل على حل كل من نطاقات العليا، مثل التي تقدمه **ICANN**.
- **OpenNIC**: هذا المشروع يتكون من شبكة من خوادم **DNS** التي تديرها **Hobbists** والمتطوعين التي تهدف إلى تقديم بنية تحتية **DNS** غير محايدة ومستقلة عن الحكومات والمنظمات ، ومجانا للجميع. يمكن لأي شخص تقديم جهاز كمبيوتر لاستخدامها كخادم **tier-2 DNS** مع شرط احترام سياسة المنظمة بشأن أمنها، والأداء، وإخفاء الهوية. بالإضافة إلى تقديم شبكة من خوادم **DNS** لـ **DNS ICANN root** القياسية، هذا الـ **DNS** يوفر أيضا مساحة بديلة للنطاقات العليا 14 [14 TLDs] ويدعم أربع نطاقات بديله **TLD** من **NewNations**، وهي المنظمة التي تقدم **domain root** لكيانات سياسية معينة مثل **Tibetan** أو الشعب الكردي.
  لمزيد من المعلومات **http://www.opennicproject.org.**

ما هو Deep Web : هو مجموعة من المواقع الغير معروفة والتي لا يتم ارشفتها في مواقع البحث ولن تجدها عند قيامك بالبحث في اي موقع بحث لأنها تستخدم نطاقات مختلفة عن التي يستخدمها الانترنت العادي فمثلا نحن نعرف النطاق **.com** و**.net** ولكن الانترنت الخفي لا يستخدم مثل هذه النطاقات بل هو يستخدم نطاقات مثل .onion و .i2p و .bit وغيرها

مثال على ذلك كالاتى:

ofrmtr2fphxkqgz3.onion

استخداماته تستخدم هذه المواقع في **black market** (السوق السوداء) مثل بيع السلاح المحتويات الجنسية ويوجد عليه العديد من مواقع الهاكرز والدروس في الهاكرز.

Darknet: هي مواقع متواجدة ولكناها لا تستخدم البروتوكولات المعروفة مثل // :http وهو يستخدم في مشاركة الملفات وعليه نستطيع ان نقول ان من يستخدم هذه المواقع هم من يقومون بممارسة الاعمال الغير مشروعة علي الانترنت وهم يستخدمون هذه المواقع لأنه لا يمكن للحكومات او اي جهة اخري بتعقبهم.

ما أهميته؟

أهمية هذا الجزء أنه أكبر بكثير من المحتوى المرئي من الانترنت ويقدر حجمه بأنه 500 ضعف محتوى الويب المرئي (الويب المرئي هو الجزء الذي يمكن الوصول إليه عن طريق محركات البحث)، ويتميز أيضا بكفاءة المعلومات الموجودة فيه وكثرتها، ولذا نفقد الكثير من المعرفة في هذا الجزء.

ما سبب أنه مخفى أو لا يمكن لمحركات البحث أن تراه؟

سمى هذا الجزء من الانترنت **invisible web** أو **deep web** لأن محركات البحث لا يمكن أن تراه أو تجده بسهولة أو ببساطة هذا المحتوى غير مصمم ليفهرس أو ليتم رؤيته على محركات البحث، ولنفهم أكثر يجب أن نعرف كيفية عمل محركات البحث:

محتوياته:

- محتويات قواعد البيانات **Databases** مثل قواعد بيانات المنشورات وأرقام التليفونات وأدلة المكتبات.
- الملفات الغير نصية كـ **PDF** والصور وملفات الورد.
- البيانات المحمية بكلمة سر
- البيانات دائمة التغيير **Dynamic data** مثل الأخبار ومواعيد رحلات الطيران.
- التعليقات على المقالات
- البيانات الموجودة في المواقع الاجتماعية **Facebook** و**Twitter**.
- الثد وينات.
- المرجعيات **Bookmarks** في مواقع مشاركة المرجعية
- أسلحة -مخدرات -دروس وبرامج هاكرز نادرة أشياء غير اخلاقية

اقول لك ان الهدف من انشاء تلك المواقع المظلمة السرية هو العمل بعيدا عن اعين الرقابة والشرطة والسلطات. الهدف غير مشروع كعقد صفقات اسلحة غاشمة او قصص وروايات ممنوعة لا يمكن نشرها على الشبكة المحلية والعالمية المعروفة. كالاتجار في المخـــــدرات الخطيرة وغيرها.

ستجد كل ما هو ممنوع وإجرامي في هذا ولا تظنون ان تلك المواقع للمتعة فقط. انها عبارة عن السوق السوداء**Black Market's**. لكل شيء لا يمكنك تخيله سوف تجد بها المواقع الاجتماعية للتواصل وبرامج الهاكر الغاشمة ومحاضراتها "طبعا كل حاجة بفلوس" ليس مجاني في هذا العالم والا فما الفائدة منه

طبعا هناك مواقع مجانية مثل: شبكات التواصل الاجتماعي كالفيس بوك، كالدردشة المجانية التي تجدها على هذا الرابط

c2hluuzwi7tuceu6.onion

من الفوائد العظيمة لهذا هو التخفي وقت الاختراق حيث عند تصفح الانترنت المظلم او الخفي تقدر تتصفح المواقع العادية بس المواقع المخفية تظهر هي الأخرى.

كيفية البحث في محتويات الانترنت الخفي:

يوجد مواقع بحث تحاول فهرسة الويب الخفي مثل الاتي:

http://infomine.ucr.edu/
http://www.completeplanet.com/index.jsp
http://vlib.org/
https://archive.org/
http://clusty.com/
http://lookahead.surfwax.com/index-2011.html

فيما يلي بعض مواقع الويب التي تحتوي على قائمه بجميع مواقع الويب الخفية dark web كالاتي:

http://deepweblinks.org/
https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web

كيفية الدخول الى الانترنت المظلم؟

لدخول الى الانترنت المظلم يجب تحميل برامج خاصة لذلك كمثال فانا استعمل جوجل كروم لتصفح الانترنت وكروم غير قادرة على تصفح نطاقات اخرى غير com.gov.net.الخ

توجه الى هذا الموقع وقوموا بتحميل المتصفح الخاص بفتح تلك المواقع (متصفح تور)

https://www.torproject.org/

حجم المتصفح 22ميجا سهل الاستخدام ويشبه موزيلا فايرفوكس بالضبط

1- بعد فك ضغط البرنامج سوف تجدون ملفا باسم **Start Tor Browser.exe**
2- قم بالضغط عليه وانتظر حتى يتم الاتصال بشبكة **Tor** التي ستعامل من خلالها مع نطاقات المواقع التي تنتهي بالامتداد**Onion**
3- انتظر دقيقة تقريبا حتى يتم الاتصال ولسوف يفتح لك المتصفح تلقائيا. عقب البحث عن شبكة تور **Tor** التي نتحدث عنها قم بعمل رفريش في المرة الاول وسوف يتم الاتصال بنجاح

من خلال هذا المتصفح الفريد من نوعه يمكنك الاتصال بشبكة الانترنت المظلم والخفي والعميق.

الحمد لله تعالى نكون هنا انتهينا من الوحدة الثانية وهي عملية جمع المعلومات

Dr. Mohammed Sobhy Teba